Comms Software Requirements Specification for

Defense Information Infrastructure Common Operating Environment

11 July 1997

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 400
Newport News, Virginia 23602

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

Comms SRS for DII-COE

Contents

This page intentionally left blank.

Section 1

Scope

1.1 Identification

This Subsystem Requirement Specification (SRS) describes Communications Services of the Defense Information Infrastructure (DII) Common Operating Environment (COE).

1.2 Communications Services Overview

The Communications Services area of the DII-COE is defined as frame work for supporting connectivity and data exchange between a given autonomous system and other autonomous systems.

1.2.1 Open Systems Interconnection (OSI) Model

A discussion of the DII Communications Services requirements necessitates a background presentation of the Open Systems Interconnection (OSI) reference model. The OSI model, portrayed in Figure 1, is the model used for data communications in the DII COE. Each of the seven layers in the model represents one or more services or protocols (a set of rules governing communications between systems), which define the functional operation of Communications between user and network elements. Each layer (with the exception of the top layer) provides services for the layer above it. This model aims at establishing open systems operation and implies standards-based implementation. It strives to permit different systems to accomplish complete interoperability and quality of operation throughout the network.

The seven layers of the OSI model are structured to facilitate independent development within each layer and to provide for changes independent of other layers. Stable international standard protocols in conformance with the OSI reference model layer definitions have been published by various standards organizations.

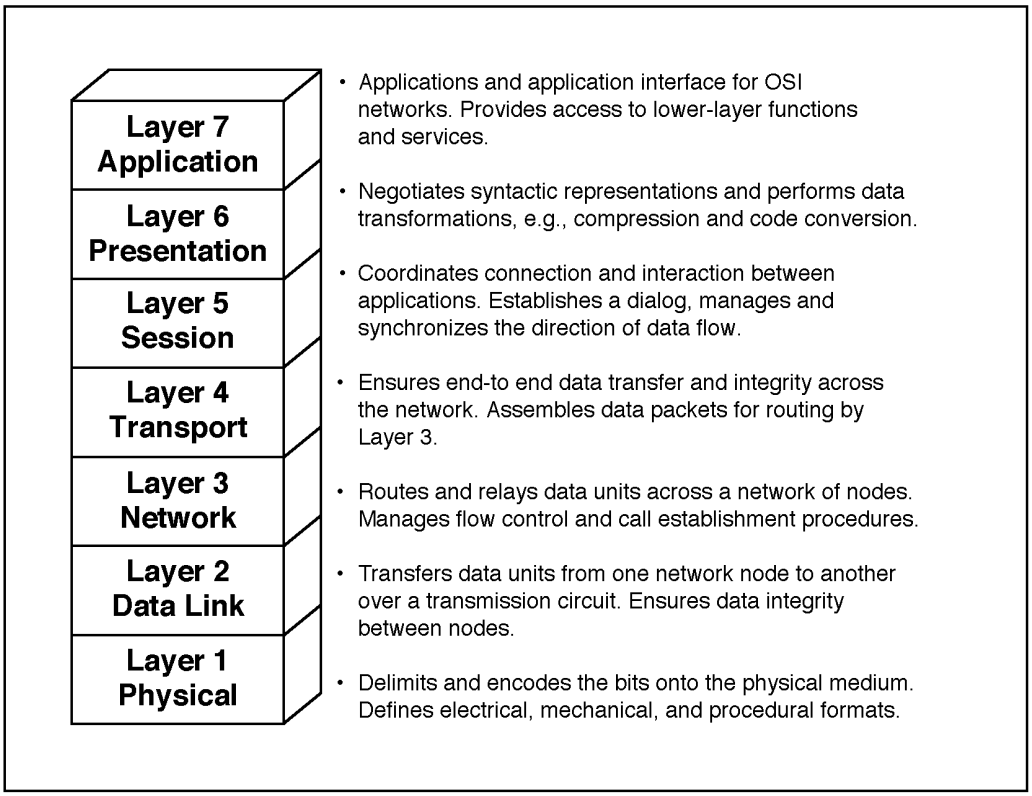

Figure 1 Open Systems Interconnection model

While the OSI model is useful for explaining the mechanics of communications, the scope of the DII COE Communication service is defined in the DoD Technical Architecture Framework for Information Management (TAFIM). The TAFIM defines communication services in the following areas:

1. Message Transfer Services
2. Voice Communications
3. Visual Services
4. Information Transfer Services
5. Information Technical Service Management
6. Network Services

1.2.2 Message Transfer Services

Message Transfer services include the following requirements:

1. Personal Message Transfer services, including the capability to send, receive, forward, store, display, and manage personal messages. This includes the capability to append attachments such as files and documents to messages.

Messages may include any combination of data, text, audio, graphics, and images and should be capable of being formatted into standard data interchange formats. This service includes the use of directories and distribution lists for routing information, the ability to assign priorities, the use of pre-formatted electronic forms, and the capability to trace the status of messages throughout the communication pipeline. Associated services include a summarized listing of incoming messages, a log of messages received and read, the ability to file or print messages, and the ability to reply to or forward messages.

2. Organizational Message Transfer services, including the capability to send, receive, forward, display, retrieve, prioritize, and manage predefined and unformatted organizational messages. Organizational messages should use standard data interchange formats and may include any combination of data, text, audio, graphics, and images. This includes the capability to review and authenticate messages. Incoming message processing services include receipt, validation, distribution, and dissemination of incoming unformatted messages based on message profiling, message precedence, and system security restrictions. Outgoing message processing services include coordination by Site's staff organizations, authorized release, and verification of record messages prior to transmission. User support services include the selection and display of messages from a message queue, on-line management of search profiles, search and retrieval of stored messages based on message content comparison to queries formulated by the analysts, and composition of record messages wrappers for transmission.

3. Enhanced telephony services, including call forwarding, call waiting, programmed directories, teleconferencing, automatic call distribution (useful for busy customer service areas), and call detail recording. Enhanced telephony service also includes precedence and preemption capabilities.

4. Shared screen services that provide audio teleconferencing with common workstation windows between two or more users. This includes the capability to refresh windows whenever someone displays new material or changes an existing display. Every user has the capability to graphically annotate or modify the shared conference window.

5. Teleconferencing services that provide two-way video or multi-port transmission between different sites. These services include:

   - full motion display of events
   - participants in a bi-directional manner
   - support for the management of directing the cameras including:
     - ranging from fixed position
     - sender directed
     - receiver directed
     - automated sound pickup

6. Broadcast services that provide one-way audio or audio/video communications

services between a sending location and multiple receiving locations. Broadcast services also includes data communications services.

- Combat Net Radio services that provide audio communications between multiple sending and receiving locations.

- Conferencing services that allow groups to participate in conferences. These conferences may not occur in real time. Conferees or invited guests can drop in or out of conferences or subconferences at will. The ability to trace the exchanges is provided. Services include exchange of documents, conference management, recording facilities, and search and retrieval capabilities.

One end of the Message Transfer service is bounded by and includes the logical system input/output devices. This does not necessarily include down-line conveyance vehicles such as cryptos, modems, radios, etc. The other end of Communication service is bounded by and includes the message collection and distribution functions supporting client applications and other service areas such as the Message Processing Services. A notional communications architecture is depicted in Figure 2. Using this definition of the Message Transfer service and its boundaries allows for a segregatable and certifiable (where appropriate) communications subsystem that can be utilized for DII COE with controlled mechanism for handling extensions and customizations of services.

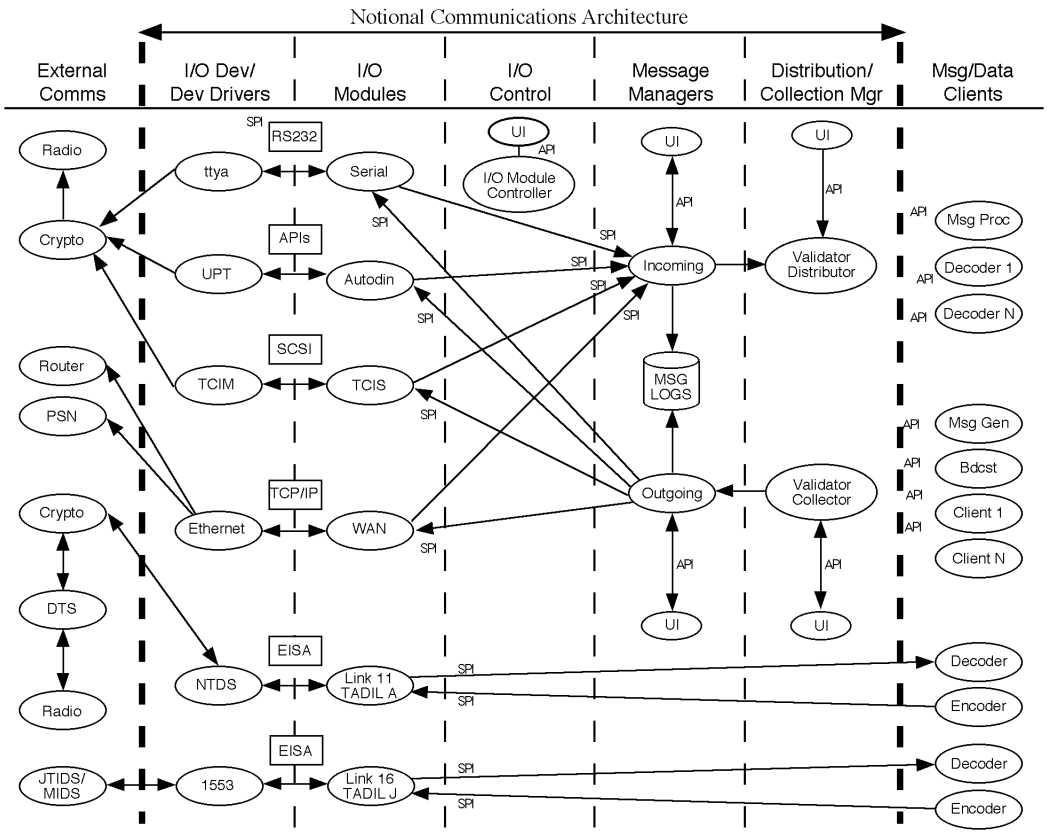

Figure 2 Notional Communications Architecture

These services allow a user to prepare, send, and receive messages. The most fundamental Message Transfer service supports text-based Message Transfer only. Increasingly more sophisticated Message Transfer services provide support for various types and formats of information in addition to text, and will include data files, graphics, facsimile, and voice. The Message Transfer services used by all DoD include two main categories:

1. The Automated Data Information Network (AUTODIN) provides the current capabilities for organizational Message Transfer services for USMTF messages.

2. The Defense Message System (DMS) will provide target capabilities for personal and organizational Message Transfer services to eventually replace AUTODIN.

However, the Message Transfer services include many other DoD service specific networks, interfaces, and protocols that provide for information transfer between sites and systems.

The term “message” refers to the logical collection of data bits bundled by applying the rules for the format of the data (character-oriented, bit-oriented, graphics, voice,

data, etc.). For example; Formatted Record messages are bounded by applying the rules of JANAP 128, ACP 126M, ACP 127, etc. Tactical Data Information Link Tactical Data Link (TADIL) binary messages are bounded by frame labels indicating the applicable series message and the fixed size of the given message. These messages are bounded by applying the rules of OS411 and OS516. A graphics for such as TIF, BMP, etc.etc has a specified format as do audio files.

Record Message Handling: This class of messages usually consists of formatted messages (military examples include OTH GOLD, USMTF, etc.) within a standard wrapper (military examples include JANAP 128, ACP 126M, etc.) Subsequent distribution of messages / data by Message Processing Software or other client applications is external to Communications service. The services provided by Message Processing Software will handle posting messages for human consumption in the appropriate electronic mail box as well as automatically processing messages for computer consumption to update system databases.

Binary Message Handling: Some communications interfaces may have client message encoders and decoders (from message processing) which will interact more directly with the interface conveying data to and from database engine(s) of the system where message logging, accounting, and other features used for record messages, do not apply. Should those features be applied they would adversely affect the timeliness and usefulness of the data. This class of messages usually consists of high speed / volume binary data which is decoded and encoded by commonly structured message / data client services and capable of interacting with other common system API structures.

Message Transfer services includes such areas as physical interfaces, protocols, interface control, data bounding into messages, message identification, message storage, message retrieval, message logging, message notification, message alerting, message queuing, message validation, message collection, and message distribution.

In postal service terms, the Message Transfer Service looks at the envelope of the message not the actual content. The envelope conveys information about the source, destination and priority of the message; whereas a user or client application handles the processing of the actual message content.

In terms of the OSI Reference Model, the DII COE Message Transfer services notional architecture (See Figure 2) can be described in terms of the 7 layer reference model (See Figure 3). In this context, client applications (layer 7) are establishing virtual connections to their counterpart applications on remote hosts via the Message Transfer services of DII COE. Data flows amongst these client applications without their direct involvement or knowledge of the underlying conveyance mechanisms. Although this model is useful for describing interfaces between open systems some difficulties are found when applying the model to older / closed system architectures that will continue to interface to DII COE. Although these older systems / interfaces are being phased out, it will still be many years before that happens. Therefore, it is important to propose a communications service solution that handles legacy as well as emerging communication technologies with an effective infrastructure that

supports simultaneous instances of these technologies.

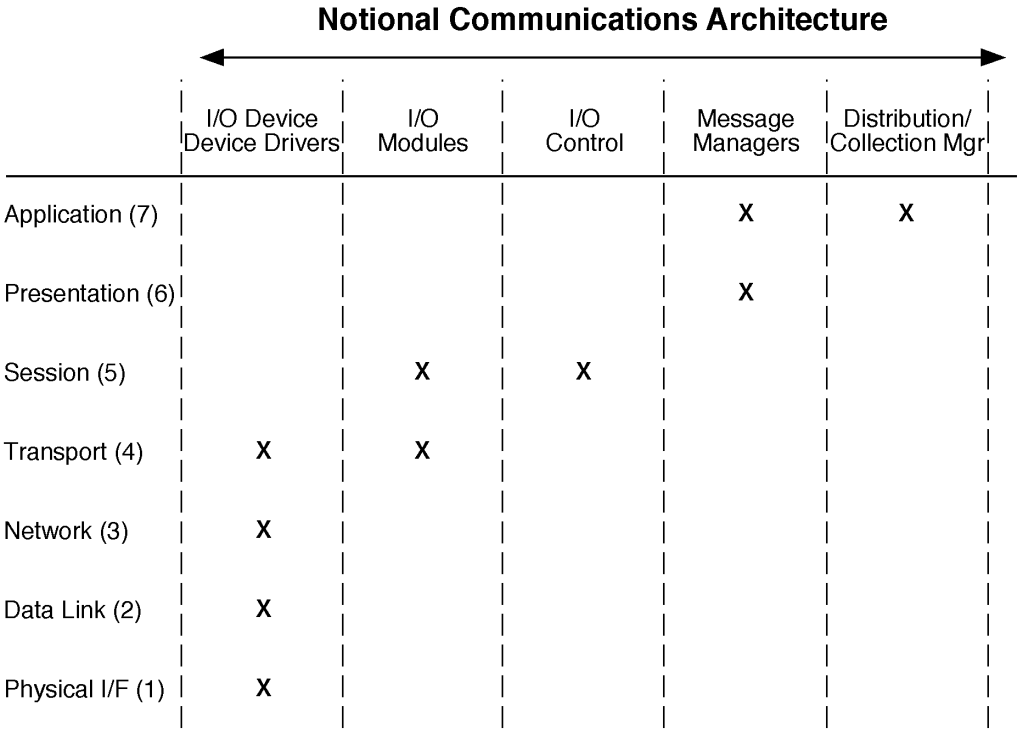

Figure 3 Notional Architecture and OSI Layers

Figure 4 presents a depiction of the relationship between Communications and Messaging and indicates at a high level how the various services interact to provide for Communications and Messaging services.

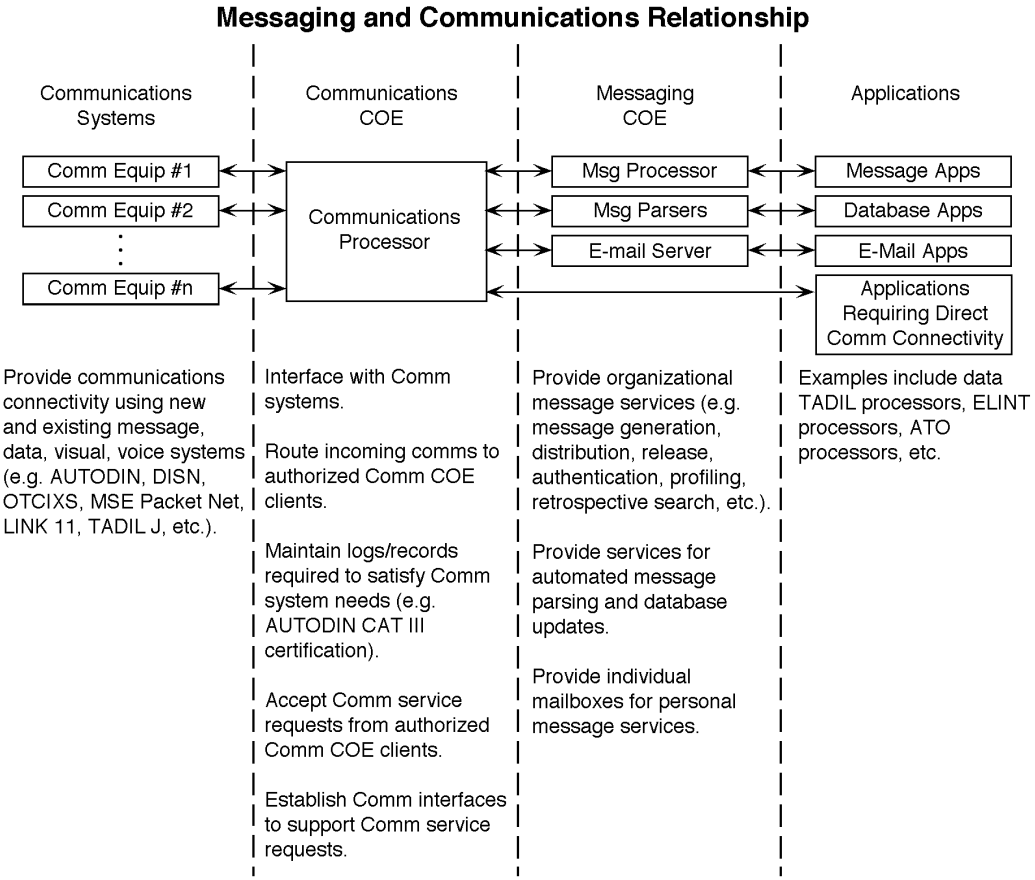

Figure 4 Nominal Communications and Messaging

1.2.3 Voice Communications

These services provide inter-human voice communications and include real-time (e.g., plain-old-telephone-service and air-to-ground) and stored voice messages. Telephone services and radio services are specialized forms of voice communications services. An overall voice communications service may actually consist of individual telephone services and radio services. The voice communications services must employ information transfer services for actual voice transmission.

1.2.4 Visual Services

These services generally provide mechanisms for capturing, processing, transferring, and displaying visual information. This service area includes imagery, video, and facsimile. The services for transferring the visual information are in addition to the

information transfer services. Visual services must employ information transfer services for actual information transmission.

1.2.5 Information Transfer (IT) Services

These services support the transfer of C4I information (e.g., voice, data, video, messages, images, etc.) between users and/or C4I systems.

1.2.6 Information Technical Service Management

Services supporting the management, integration, accounting, and security of the other IT Services and the systems, facilities, and resources comprising those services. This service includes specific services such as network management, message management, and electronic key management.

1.2.7 Network Services

Network services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous networked environments. They include the following functional areas:

1. **Data communications**, which include protocols for reliable, transparent, end-to-end data transmission across communications networks.

2. **Personal/microcomputer support** for interoperability with systems based on a variety of operating systems.

1.2.7.1 Internet Protocol Suite (IPS)

The Internet Protocol Suite (IPS) is based on the Internet Protocol (IP) and Transmission Control Protocol (TCP), which were developed within the U.S. military-funded research establishment and have since grown to become the basis of the worldwide Internet, is generally referred to as the TCP/IP Protocol Suite. Standardization of the IPS is carried out by the Internet Engineering Task Force (IETF).

The IPS, although neither required nor precluded by GOSIP, is widely used by Federal agencies. Today there is significantly more actual interoperation within and between Federal agencies using IPS than using OSI standards, as well as between Federal agencies and the public. The Profile for Open Systems Internetting Technologies (POSIT) as described in FIPS Publication 146.2 and the Government Network Management Profile (GNMP) as described in FIPS Publications 179.1 have been selected as the guidance documents for internet access.

1.2.7.2 The GCCS COE Network Services shall use the TCP/IP.

1.3 Document Overview

Section 1	Identifies the communications functional area of the DII COE.
Section 2	Lists any documents either referenced within, or applicable to, this document.
Section 3	Specifies the functional requirements of the communications area, including tracing to source documentation and candidate implementation designs.
Section 4	Specifies the quality assurance methods necessary to ensure that the functional requirements have been met.
Section 5	Identifies the requirements for the preparation of the modules associated with the communications area.
Section 6	Identifies the integration approach and risk assessment, a prioritized list of functional requirements, as well as a schedule for implementation of all functional requirements.

Section 2

Applicable Documents

This section references to applicable documents that describe requirements, specifications, and functional capabilities for this area.

2.1 Government Documents

- Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Preliminary Version 3.2, DISA, 11 July 1997
- DISA Communications Architecture; DISA TAFIM 700, Vol. 2
- CJCSM 6231, Manual for Employing Joint Tactical Communications, Vol. 1-7
- MIL-STD 188-220A, Interoperability Standard for Digital Message Transfer Device Subsystems, 28 April 95
- CM-500-62-02, GCCS User Interface Specification (Style Guide), Version 1.0, 1 Oct. 1994
- MIL-STD 188-114A, Electrical Characteristics of Digital Interface Circuits, 13 Dec. 1991
- MIL-STD 188-110A, Interoperability and Performance Standards for Data Modems, 30 Sep. 1991
- MIL-STD-188-171, Interoperability Standards for Information and Record Traffic Exchange (Mode I), 19 May 1989
- MIL-STD-188-172, Interoperability Standards for Information and Record Traffic Exchange (Mode II), 7 Dec. 1989
- MIL-STD 188-220, Interoperability Standard for Digital Message Transfer Device Subsystems, 1993
- MIL-STD 188-530
- MIL-STD-1553B, Aircraft Internal Time Division Command/Response Multiplex

Data Bus, 21 Sep. 1978

- MIL-STD-1397A
- MIL-STD-188-203-1A, Interoperability and Performance Standards for Tactical Digital Link (TADIL) A, 8 Jan. 1988
- MIL-STD 6016A (TADIL J)
- NRaD, User Interface Specifications for Navy Command and Control Systems, Version 1.3, November, 1993
- FIPS Publication 146.2 Profile for Open Systems Internetting Technologies (POSIT)
- FIPS Publication 151-2
- FIPS Publication 179.1 Government Network Management Profile
- Army, C4I Technical Architecture, Version 3.0, 22 March 1996
- Operational Specification for TADIL A (0S45411.2)
- Operational Specification for TADIL J (0S5511.1)
- FIPS PUB 145: Government Open Systems Interconnection Profile (GOSIP), 24 August 1988
- FIPS PUB 145-1: GOSIP Version 2.0, April 1989
- NIST 500-177: Stable Implementation Agreement System Interconnection Protocol, Version 2, Edition 1, December 1988
- NISTIB 88-3824-2: Ongoing Implementation Agreement for Open Systems Interconnection Protocols: Continuing Agreement, December 1988

2.2 Non-Government Documents

- ISO / IEC JTC1 IS 7498:1986: Management Framework
- ISO / IEC JTC1 IS 8326:1987 and 8327:1987: Connection-Oriented Session Service and Connection-Oriented Session Protocol, respectively
- ISO / IEC JTC1 8326 AD 2: Connection-Oriented Session Service - Incorporation of Unlimited User Data
- ISO / IEC JTC1 8327 AD 2: Connection-Oriented Session Protocol - Incorporation of Unlimited User Data

- ISO / IEC JTC1 IS 8571:1988: File Transfer, Access, and Management (FTAM), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if File transfer, Access, and Management functionality are required
- ISO / IEC JTC1 IS 8822:1988 and 8823:1988: Connection-Oriented Presentation Service and Connection-Oriented Presentation Protocol, respectively
- ISO / IEC JTC1 IS 8824:1987: Abstract Syntax Notation 1 (ASN.1)
- ISO / IEC JTC1 IS 8825:1987: Basic Encoding Rules (BER) for ASN.1
- ISO / IEC JTC1 IS 9041:1990 (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required
- ISO / IEC JTC1 IS 9072-1:1989 and 9072-2:1989: Remote Operations Service Element (ROSE) and Remote Operations Protocol (ROP), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES) and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5
- ISO / IEC JTC1 IS 10165-1:1991: Structure of Management Information (SMI)
- ISO / IEC JTC1 IS 10165-2:1991: Definition of Management Information (DMI)
- ISO / IEC JTC1 IS 10165-4:1991: Guidelines for the Definition of Managed Objects (GDMO)
- CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required
- Network Management Forum: OMNIPoints 1
- NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7, of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-162)
- Open software Foundation Distributed Computer Environment (DCE): Remote Procedure Call (RPC) Service Definition
- IEEE P1327 Object Management API
- X / Open's XOM
- ISO 7498, OSI Basic Reference Model
- ISO 7776, LAPB

- ISO 9314, FDDI
- ATM
- AALS
- Packet Switching
- STD-5, Internetwork Protocol (IP)
- STD-6, UDP
- STD-7, Transport Control Protocol (TCP)
- STD-8, TELNET
- STD-9, File Transfer Protocol (FTP)
- STD-10, Simple Mail Transport Protocol (SMTP)
- STD-13, Domain Name Service (DNS)
- STD-15, Simple Network Management Protocol (SNMP)
- X.400 / X.500
- IEEE POSIX, Protocol Independent Interfaces, IEEE P1003.1G, 1995
- IEEE 802.2, LLC, IEEE, 1985
- IEEE 802.3, IEEE, 1985
- RS232
- RS422
- RS423
- RS449
- RS530
- RFC-951, BOOTP
- RFC-1541, DHCP
- RFC-1583, OSPF v2

- RFC-1654, BGP v4
- RFC-1661, Point-to-Point Protocol (PPP)
- ANSI X.131-1986 (SCSI)
- XTI, X/Open Transport Interface, X/Open Foundation
- Network Provider Interface, AT&T, Version 1.2
- UNIX System V.4 Programmer's Guide, Networking Interfaces
- UNIX System V.4, Network Programmer's Guide
- Distributed Computing Environment (DCE)
- Interface Design Document (IDD) for the Tactical Communications Interface Module (TCIM) Common Interface Software (TCIS) to Applications Software, IDD-0288-S001, Rev. L, 23 June 1995
- INRI, Software Requirement Specification for the Unified Build 2.1, 21 July 1994
- INRI, Communications Service Applications Programmer's Interface
- INRI, Software Architecture Guide for the Unified Build
- CASS Communications Server Software User's Manual, N250-92-L029-008, 1992
- CASS Communications Server Interface Description Document, N250-92-L029-009, 1992
- CASS Communications Server Software Requirements Specification, N250-94-L119-010, 1994
- ISO 7498-1984: Information Processing Systems, Open Systems Interconnection, Basic Reference Model
- ISO 7498 AD 1-1987: Information Processing Systems, Open Systems Interconnection, Basic Reference Model, Addendum 1: Connectionless Mode Transmissions
- ISO 7498-2-1989: Information Processing Systems, Open Systems Interconnection, Basic Reference Model, Part 2: Security Architecture
- ISO 7498-3-1989: Information Processing Systems, Open Systems Interconnection, Basic Reference Model, Part 3: Naming and Addressing

- ISO 7498-4-1989: Information Processing Systems, Open Systems Interconnection, Basic Reference Model, Part 4: Management Framework
- ISO 8509-1987: Information Processing Systems, Open Systems Interconnection, Service Conventions
- ISO DIS 9545-1989: Information Processing Systems, Open Systems Interconnection Application Layer Structure
- Tanenbaum, Andrew s. “Computer Networks,” Prentice Hall, 1989.

Section 3

Requirements

3.1 Message Transfer Services Requirement Overview

The Message Transfer Service Requirements have been divided into 5 conceptual areas that comprise a notional Comms Message Transfer subsystem architecture (See Figure 2):

- I/O devices
- I/O interfaces
- Interface control
- Message management
- Distribution and Collection management

General requirements for DII COE Comms Service are listed first followed by requirements specific to a given domain (e.g. C4I, EC, logistics, etc.)

3.2 Message Transfer Services Requirements

3.2.1 General Requirements

3.2.1.1 Modules wishing to use Message Transfer Services must be written as clients to the Communication server.

3.2.1.2 Message Transfer Services shall support 24-Hour, 7 day per week operations.

3.2.1.3 Message Transfer Services shall provide for system restart to normal operations with no message loss after elimination or correction of a system malfunction or failure condition.

3.2.1.4 Message Transfer Services shall not be held responsible for queuing delays on external circuits. In the event that a message cannot be delivered when it is ready for delivery due to circumstances beyond the Communications processor's control, Message Transfer Services shall queue the message for later delivery.

3.2.1.5 Message Transfer Services shall be capable of handling both individual and organizational messages. This includes not only record (character-oriented and formatted) and binary messages but also electronic mail (E-mail).

3.2.1.6 Message Transfer Services shall include message handling functions for storage.

3.2.1.7 Message Transfer Services shall include message handling functions for retrieval.

3.2.1.8 Message Transfer Services shall include message handling functions for query.

3.2.1.9 Message Transfer Services shall include message handling functions for printing.

3.2.2 Input/Output Devices Requirements

3.2.2.1 Message Transfer Services shall be able to use device drivers provided by the COE and/or install the required operating system drivers to support data transfer.

3.2.2.2 Serial Device Requirements

Message Transfer Services shall be capable of connecting Data Terminal Equipment (DTE) or Data communications Equipment (DCE) such as terminals, personal computers, modems or mainframe host computers. The following data communications capabilities shall be supported:

3.2.2.2.1 Message Transfer Services shall support Asynchronous Serial Interfaces.

3.2.2.2.2 Message Transfer Services shall support Synchronous Serial Interfaces.

3.2.2.2.3 Message Transfer Services shall support Direct Connection of DTE's and DCE's via RS 232-D interfaces.

3.2.2.3 Parallel Device Requirements

Message Transfer Services shall be capable of interacting with a parallel device and driver.

3.2.2.4 Network Device Requirements.

Message Transfer Services shall be capable of interacting with a network device and driver.

3.2.2.5 Message Transfer Services shall support external SCSI devices used for communications devices or other communications uses.

3.2.2.6 Message Transfer Services shall support VME/VXI boards to be used for communications processors, communications multiplexers, or other communications uses.

3.2.2.7 Message Transfer Services shall support EISA boards to be used for communications processors, communications multiplexers, or other communications uses.

3.2.2.8 Message Transfer Services shall support S-Bus boards used for communications processors, communications multiplexers, or other communications uses.

3.2.2.9 Message Transfer Services shall support PCMCIA cards used for communications processors, communications multiplexers, or other communications uses.

3.2.2.10 Message Transfer Services shall support PCI bus-based devices for communications processors, communications multiplexers, or other communications uses.

3.2.2.11 Message Transfer Services shall support Universal Serial Bus (USB) bus-based devices for communications processors, communications multiplexers, or other communications uses.

3.2.3 Input/Output Interfaces Requirements

3.2.3.1 An interface definition shall be provided to support the addition of interfaces as "plug in" modules to the communication server architecture.

3.2.3.2 Serial Interface

3.2.3.2.1 Message Transfer Services shall provide an interface to transmit and receive messages via serial EIA-RS-232.

3.2.3.2.2 Message Transfer Services shall provide an interface to transmit and receive messages via serial MIL-STD-188.

3.2.3.2.3 Message Transfer Services shall provide an interface to transmit and receive messages via serial EIA-RS-449.

3.2.3.2.4 Message Transfer Services shall provide an interface to transmit and receive messages via serial V.35.

3.2.3.2.5 Message Transfer Services shall support the AUTODIN Mode 1 protocol and interface.

3.2.3.2.6 Message Transfer Services shall support the AUTODIN Mode 2 protocol and interface.

3.2.3.2.7 Message Transfer Services shall support the AUTODIN Mode 6 protocol and interface.

3.2.3.2.8 Message Transfer Services shall provide an interface to transmit and receive messages via Kermit.

3.2.3.2.9 Message Transfer Services shall provide an interface to transmit and receive messages via PPP.

3.2.3.2.10 Message Transfer Services shall provide an interface to transmit and receive messages via XModem.

3.2.3.2.11 Message Transfer Services shall provide an interface to transmit and receive messages via YModem.

3.2.3.2.12 Message Transfer Services shall provide an interface to transmit and receive messages via ZModem.

3.2.3.3 Message Transfer Services shall provide an interface to transmit and receive messages via floppy disk.

3.2.3.4 Message Transfer Services shall provide an interface to transmit and receive messages via network disk directories.

3.2.3.5 Network Interfaces

3.2.3.5.1 DII COE networks shall be based on Ethernet standards (IEEE 802.2, 802.3, 802.4, 802.5), with Fiber Distributed Data Interface (FDDI) backbones to support larger installations.

3.2.3.5.2 Hardware components shall be compatible with the ISO 8802-3 (IEEE 802.3) specification.

3.2.3.5.3 MIL-STD-187-700 (Interoperability and Performance Standards for the Defense Information System) shall be used to share digital information across common user communication systems.

3.2.3.5.4 Message Transfer Services shall provide an interface to transmit and receive messages via Transmission Control Protocol / Internet Protocol (TCP / IP) network communications.

3.2.3.5.5 Each layer of the implemented protocol stacks shall be functionally autonomous from any adjacent layer.

3.2.3.5.6 Message Transfer Services shall provide an interface to transmit and receive messages via broadcast User Datagram Protocol/Internet Protocol (UDP/IP).

3.2.3.5.7 Message Transfer Services shall provide an interface to transmit and receive messages via multicast UDP/IP.

3.2.3.5.8 Message Transfer Services shall provide an interface to transmit and receive messages via network file transfer protocol (ftp).

3.2.3.5.9 Message Transfer Services shall provide an interface to transmit and receive messages via trivial network file transfer protocol (tftp).

3.2.3.5.10 Message Transfer Services shall provide an interface to transmit and receive messages via IPX/SX network communications.

3.2.3.5.11 Message Transfer Services shall provide an interface to transmit and receive messages via Banyan Vines network communications.

3.2.3.6 Email Interface

3.2.3.6.1 Message Transfer Services shall provide an interface to transmit and receive messages via network Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail).

3.2.3.6.2 Message Transfer Services shall provide an interface to transmit and receive messages via X.400 mail (E-mail).

3.2.3.6.3 Message Transfer Services shall provide an interface to receive messages via Post-Office-Protocol Version 3 (POP-3) E-mail.

3.2.3.6.4 Message Transfer Services shall provide an interface to receive messages via IMAP-4 E-mail.

3.2.4 Input/Output Interface Control

3.2.4.1 Message Transfer Services shall provide the user interface to monitor the status and data flow through all communication interfaces within a given suite.

3.2.4.2 Message Transfer Services shall provide default user interface clients to interact with the various Message Transfer Services for the creation, deletion, activation, deactivation, and configuration of communications interfaces, messages, logs, etc. These client applications will use the defined APIs of the system services and provide the basic capabilities for exercising the various aspects of Communication subsystem without the presence of other service areas/client applications.

3.2.4.3 Message Transfer Services shall not impose an arbitrary message size limit.

Message sizes and rules for segmentation / collation shall be determined by the Interface and message sources. Any packetization will be transparent to the Message Transfer Services user.

3.2.4.4 Message Transfer Services shall provide the capability to perform a controlled (normal) termination of any or all communications which are active.

3.2.4.5 Message Transfer Services shall provide channel status and utilization information on request of an application program; channel status will include successful transmission count, aborted transmission count, received message segments with not correctable error(s) count.

3.2.4.6 Message Transfer Services shall provide a framework and toolkit for Interface developers that allows a new interface to be plugged into the system without modifying the Message Transfer Services code.

3.2.5 Message Management Requirements

3.2.5.1 Message Bounding: Message Transfer Services shall provide a configurable and extensible mechanism for specifying message or data bounding criteria to be used by various interfaces in the handling of message traffic.

3.2.5.1.1 Message Transfer Services shall be able to bound messages using the rules of the JANAP 128 message envelope type.

3.2.5.1.2 Message Transfer Services shall be able to bound messages using the rules of the ACP 123 message envelope type.

3.2.5.1.3 Message Transfer Services shall be able to bound messages using the rules of the ACP 126M message envelope type.

3.2.5.1.4 Message Transfer Services shall be able to bound messages using the rules of the ACP 127 (NATO) message envelope type.

3.2.5.1.5 Message Transfer Services shall be able to bound messages using the rules of the DD173 message envelope type.

3.2.5.1.6 Message Transfer Services shall be able to bound messages using the rules of the DOI 103 message envelope type.

3.2.5.2 Message Identification: Message Transfer Services shall provide a configurable and extensible mechanism for specifying message format and message type identification criteria to all for the message format / type labeling of current and future messages.

3.2.5.3 Message Logging

3.2.5.3.1 Message Transfer Services shall provide a mechanism for the logging

of transmitted or received messages by message type.

3.2.5.3.2 Message Transfer Services shall provide a mechanism for the logging of transmitted or received messages by classification.

3.2.5.3.3 Message Transfer Services shall provide a mechanism for the logging of transmitted or received messages by precedence.

3.2.5.3.4 Message Transfer Services shall provide a mechanism for the logging of transmitted or received messages by Date-Time-Group (DTG).

3.2.5.3.5 Message Transfer Services shall provide a mechanism for viewing messages that have been logged.

3.2.5.3.6 Message Transfer Services shall provide a mechanism for correcting messages that have been logged.

3.2.5.3.7 Message Transfer Services shall provide a mechanism for editing messages that have been logged.

3.2.5.3.8 Message Transfer Services shall provide a mechanism for reprocessing messages that have been logged.

3.2.5.3.9 Message Transfer Services shall provide a mechanism for retransmitting messages that have been logged.

3.2.5.3.10 Message Transfer Services will retain a copy of original messages that have been edited.

3.2.5.3.11 Message Transfer Services shall support creation, deletion, and management of multiple message logs on both incoming and outgoing traffic allowing for the segregation of messages into different logs based on message type, or other criteria.

3.2.5.3.12 Message Storage / Retrieval: Message Transfer Services shall provide a mechanism for the storage and retrieval of messages or data transmitted to or received from an interface for a period appropriate to the interface and system capacity.

3.2.5.3.13 Message Archive / Retrieval: Message Transfer Services shall provide a mechanism for the long term storage and retrieval of up to a year's worth of messages and logs to off-line media.

3.2.5.4 Precedence Queuing

3.2.5.4.1 Messages shall be processed on a first-in, first-out (FIFO) basis, by precedence. The highest precedence queued messages shall be processed before any lower precedence queued messages, regardless of their order of

arrival.

3.2.5.4.2 Lower precedence messages shall be preempted (busted) by flash or ECP precedence messages on all circuits capable of message cancellation.

3.2.5.5 Message Management APIs

3.2.5.5.1 Message Transfer Services shall provide APIs to the Message Processing module allowing client applications to manipulate messages through these APIs.

3.2.5.5.2 Message Transfer Services Message Management APIs will support C, C++, and Ada client applications.

3.2.5.5.3 Message Transfer Services shall provide APIs to construct the message header information independent of constructing the message body.

3.2.6 Message Distribution / Collection / Validation

3.2.6.1 Message Transfer Services shall provide a mechanism for message processing client applications to request notification for messages of interest.

3.2.6.2 Message Transfer Services shall provide a mechanism for message processing client applications to request alerting for messages of interest by various criteria such as message type, precedence, etc.

3.2.6.3 Addressee Database

3.2.6.3.1 Message Transfer Services shall support a database of addressees, which shall be maintained on nonvolatile storage and a backup for the addressee database will be provided.

3.2.6.3.2 Message Transfer Services shall provide a method for the comms administrator to change the addressee database on-line. Changes made by the operator shall persist over a system restart.

3.2.6.3.3 Message Transfer Services shall allow the operator to add addressees and their routing destinations.

3.2.6.3.4 Message Transfer Services shall allow the operator to correct addressees and their routing destinations.

3.2.6.3.5 Message Transfer Services shall support a Plain Language Addressees (PLA) database capable of storing PLA, Address Indicator Groups (AIG), Office Codes, and routing indicators (RI) associated with them.

3.2.6.4 Message Validation

3.2.6.4.1 Message Transfer Services shall provide a mechanism for the validation of message headers and types on both incoming and outgoing traffic.

3.2.6.4.2 Message Transfer Services shall provide a mechanism for the logging of messages with invalid formats.

3.2.6.4.3 Message Transfer Services shall provide a mechanism for the operator notification of messages with invalid formats.

3.2.6.4.4 Message Transfer Services shall provide a mechanism for the correction of messages with invalid formats.

3.2.6.4.5 Message Transfer Services shall provide a mechanism for the reprocessing of messages with invalid formats.

3.2.6.4.6 The message error type shall be displayed in its original form and in plain English form.

3.2.6.5 Message Accountability

Message accountability is the real-time capability to prevent unrecoverable message loss or error and the off-line capability to identify the location and potential cause of message loss.

Message output capability is the capability to deliver valid received messages to the output destination system.

3.2.6.5.1 Message Transfer Services shall provide a message input accountability of 99.999% with an objective of 100% of messages handled over interfaces that support protocol acknowledgment.

3.2.6.5.2 Message Transfer Services shall provide a message output accountability of 99.999% with an objective of 100% of messages handled over interfaces that support acknowledgment.

3.2.6.5.3 Message accountability functions shall be performed automatically within Message Transfer Services.

3.2.6.5.4 Message Transfer Services shall provide error detection to ensure message accountability as messages and data are processed from one device to another. Operator notification shall be provided for all errors detected.

3.2.6.6 Retrospective Search

3.2.6.6.1 Provide users the capability to search the message journal retrospectively for the messages of interest based on defined search criteria against the complete message and any annotations.

3.2.6.6.2 Provide processes the capability to search the message journal retrospectively for the messages of interest based on defined search criteria against the complete message and any annotations.

3.2.6.6.3 Provide the user the ability to enter search interactively via a user interface.

3.2.6.6.4 Provide the user the ability to enter delivery information interactively via a user interface.

3.2.6.6.5 Provide the user the ability to enter search via an API.

3.2.6.6.6 Provide the user the ability to enter delivery information via an API.

3.2.6.6.7 Have no set limit on the maximum number of searches that can be run against a particular message.

3.2.6.6.8 Have no set limit on the maximum number of users or processes to which results of a search can be sent.

3.2.6.7 Operational Journal

Message Transfer Services shall provide an area where both inbound and outbound messages are filed. Records placed in the operational journal will be accessible by authorized users for retrieval, annotation, and / or additional processing. The operational journal shall:

3.2.6.7.1 Provide the capability to generate / display directory of journal records

3.2.6.7.2 Provide the capability to log the following information from received and transmitted messages:

a. Date and time of message origination - Date Time Group (DTG)

b. Date and time the message was received

c. Subject / Message ID

d. Message originator

e. Message destination

f. Security classification (including codewords / nicknames and special handling)

g. Message identification

h. Message Sequence number

i. Message transmission / reception status

3.2.6.7.3 Provide the capability to selectively log the following information from received and transmitted messages at the request of an application program:

a. Message sender
b. Message type
c. Time Received
d. Message Time Stamp
e. Channel
f. Status

3.2.6.7.4 Provide the capability to selectively retrieve the logged message information.

3.2.6.7.5 Provide the capability to maintain the status of all messages under coordination and release review.

3.2.6.7.6 Provide the capability for members on the message coordination and release list to access the status of all messages under coordination.

3.2.6.7.7 Provide the capability to store the contents of the receive queue for subsequent retrieval in the event of a W / S re-initialization.

3.2.6.7.8 Provide the capability to store selected messages on-line for quick access. Storage parameters shall include the message profile (i.e., type, originator, precedence) and specified time period (i.e., for 1, 2, 6, 12, 24, and 48 hours).

3.2.6.7.9 Provide the capability to search the message storage for messages of interest based upon a user-defined set of search criteria.

3.2.6.7.10 Provide the capability to define message storage space capacity and threshold depletion limits.

3.2.6.7.11 Message Transfer Services shall not impose an arbitrary message log limit but will base the limit on system resources (e.g., hard disk space, memory, etc.).

3.2.6.7.12 Provide the capability to monitor message storage space for depletion.

3.2.6.7.13 Provide the capability to route messages to an alternate, selectable, device when the message storage area limits are reached.

3.2.6.7.14 Provide the capability to disable the acceptance of incoming non-ECP and non-Flash messages when primary storage devices are full.

3.2.6.7.15 Provide the capability to delete the oldest messages having the same or lower precedence as the incoming message in order to make room when the message storage area is full and acceptance of incoming messages is not disabled.

3.2.6.7.16 Provide the capability to enable the acceptance (for storage) of incoming messages according to message precedence.

3.2.6.7.17 Provide the capability for an application program to delete selected messages from the message storage area.

3.2.6.7.18 Message transfer services shall provide a mechanism for validation of message formats and types on both incoming and outgoing message traffic.

3.2.6.7.19 Message Transfer Services shall provide the capability to create, store, and maintain subscriber tables.

3.2.6.7.20 Message Transfer Services shall provide the capability to extract default message relaying information from an application directory or from current network configuration and status information.

3.2.6.8 Multi-Sectioned Messages

Message Transfer Services shall be capable of supporting the message processing module requirement that messages released to it for transmission are independent of any interface or protocol's size limitations. Message Transfer Services shall therefore provide message segmentation and collation functions to break apart long messages for transmission and reassemble those message segments upon reception. Additionally, the Message Transfer Services shall:

3.2.6.8.1 Create a single message from all sections of a multi-part message received in an operator-setable time period.

3.2.6.8.2 Create multiple sections from a single message inserting the necessary segmenting information into the message body as defined by the interface specification that supports segmentation.

3.2.6.8.3 Handle an incomplete sectioned message at user direction.

3.2.6.8.4 Ensure that the message is displayed in section order regardless of whether sections are received out-of-sequence or are missing.

3.2.6.8.5 Place San indicator in the reconstituted message where portions of the message / message text are missing.

3.2.6.9 Core Incoming Message Management Requirements

3.2.6.9.1 Message Transfer Services shall provide message formatting and conversion, message in-processing, to include the viewing, logging, profiling, precedence processing, and user notification of incoming message traffic (based on message bounding).

3.2.6.9.2 Message Transfer Services shall provide for message dissemination to include distribution by precedence, distribution by profile, and distribution by mailing list.

3.2.6.9.3 Message Auto Print: Message Transfer Services shall provide a mechanism for automatically printing messages or data based on various criteria such as source, addressee, and message type.

3.2.6.9.4 Message Transfer Services shall allow the operator to perform service message handling support.

3.2.6.10 Message Routing / Auto Forward / Distribution

3.2.6.10.1 Message Transfer Services shall provide a mechanism to automatically forward messages or data to other destinations based on various criteria of the message (e.g., source, addressee, message type).

3.2.6.10.2 Message Transfer Services shall provide a mechanism for distribution of messages to back-end clients based on criteria such as message type, routing indicators, office codes, and key words. This distribution shall support the Message Processing Services.

3.2.6.10.3 Message Transfer Services shall allow the operator to add criteria for how messages are distributed to back-end users.

3.2.6.10.4 Message Transfer Services shall allow the operator to modify criteria by which messages are distributed to back-end users.

3.2.6.10.5 Message Transfer Services shall route messages based on addressees found within the message. This applies to all message bounding types.

3.2.6.10.6 Message Transfer Services shall provide the option of routing message traffic to an alternate destination based on precedence.

3.2.6.10.7 Message Transfer Services shall provide the option of routing message traffic to an alternate destination based on other message header fields as required.

3.2.6.10.8 Message Transfer Services shall provide the option of routing message traffic to an alternate destination based on routing indicators.

3.2.6.10.9 Message Transfer Services shall provide the option of routing message traffic to an alternate destination based on classification.

3.2.6.10.10 For sectionalized messages, Message Transfer Services shall provide the capability to transfer concatenated messages (i.e., the message segments are combined back into the original message) or transfer the message segments depending on the request from an application program.

3.2.6.10.11 Message Envelope Format Conversion: Message Transfer Services shall provide a mechanism for the conversion of certain message envelope formats to other message envelope formats as is appropriate for the transmission interface, for example if autoforwarding over a different type of channel that supports a different message envelope.

3.2.6.11 Message Profiling

Messages entering the message processing module must be examined to identify and/or extract (copy or demarcate) message elements. Elements extracted from messages are necessary for construction of corresponding message summaries which shall provide "two-level" message review capabilities required for distribution, coordination, and retrieval functions used during search and retrieval processes. The message processing module shall:

3.2.6.11.1 Provide the capability to enter message selection profiles for individual users, group of users, or processes.

3.2.6.11.2 Support distribution criteria to include message routing criteria or message content.

3.2.6.11.3 Compare messages and system profiles to determine which accounts should receive a copy of the associated message summaries.

3.2.6.11.4 Compare messages and system profiles to determine which accounts should receive a copy of the associated parsed data.

3.2.6.11.5 Determine from user profiles and message content which organization is assigned Action for the Office of Primary Interest (ACT/PI) for a given message.

3.2.6.11.6 Determine from user profiles and message content which account shall be designated the Action Officer (AO) for the message.

3.2.6.11.7 Provide an optional capability to distribute message summaries of transmitted messages (come-back copies) to any combination of accounts listed in the internal distribution fields (drafter, coordinators, releaser).

3.2.6.11.8 Provide an optional capability to distribute message come-back copies to any combination of accounts listed in the internal distribution fields

(drafter, coordinators, releaser).

3.2.6.11.9 Support user re-addressal of received messages for retransmission to external organizations.

3.2.6.11.10 To support generation of a message profile the Message Transfer Services shall:

a. Extract the following precedence markings (on messages so marked):

- CRITIC
- EMERGENCY COMMAND PRECEDENCE (ECP)
- FLASH
- IMMEDIATE
- PRIORITY
- ROUTINE

b. Process the message wrapper to identify and extract the following message elements:

- Subject / Message ID
- Date-Time-Group (DTG)
- Message Addresses (both action and information)
- Office Symbols (including multiple office symbols in a single address)
- Message Originator

c. Extract U.S. classification and caveat markings including, but not limited to:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- UNCLAS EFTO FOUO
- UNCLAS EFTO
- UNCLAS

d. Identify message handling markings for control functions used to enforce user “need-to-know” access within the various classification and caveat levels including, but not limited to:

- LIMDIS
- EYES ONLY (and who for)
- PERSONAL FOR (and who the message is personal for)
- SPECAT
- SPECAT EXCLUSIVE
- specified, special compartmental caveats as may be modified by the user.

3.2.6.12 Core Outgoing Message Management Requirements

3.2.6.12.1 Message Transfer Services shall provide for message out-processing to include transmittal, retransmittal, forwarding, logging, precedence processing, and review and release of messages.

3.2.6.12.2 Alternate Channel Selection / Routing: Message Transfer Services shall provide the capability for manually and automatically routing outgoing traffic from one interface to another within the constraints of the alternate routing tables.

3.2.6.12.3 Message Transfer Services shall provide a mechanism for releasing / transmitting messages or data. This mechanism will support both automatic and manual destination selection.

3.2.6.12.4 Message Transfer Services shall provide the capability to support a number of addressees per message appropriate to the interface.

3.2.6.12.5 Message Transfer Services shall provide the capability for an application program to define, without taking a workstation off-line, an alternate channel for retransmission if the retry count for data transmission is exceeded, consistent with the security level of the alternate channel and connected workstation.

3.2.6.12.6 In the event the allowable retry count is reached during data transmission over a channel, Message Transfer Services shall provide the capability to automatically attempt to utilize the assigned alternate channel for transmission.

3.2.6.12.7 Message Transfer Services shall provide the capability to define the number of recovery retries to be made in the event of failure during transmission, prior to selection of an alternate channel.

3.2.6.12.8 The output of Message Transfer Services for character-oriented messages shall be messages or data that will be passed to other functions or processes to do message parsing and subsequent update of the system's database engine(s).

3.2.6.12.9 Message Transfer Services shall provide the capability to notify an application program in case of a rejected or abort transmission after recovery and retry mechanisms have been exhausted.

3.2.6.12.10 Message Transfer Services shall support generation of simulated message traffic during exercises and training.

3.2.6.12.11 Message Transfer Services shall notify the Application or Higher Layer software via APIs regarding message reception, message notification, and status but shall not be limited to the following:

a. Transmission notification such as successful or not successful.

b. Message reception status such as acknowledge or negative acknowledgment (ACK/NACK)

c. Message reception error notification

d. Configuration status

3.3 Voice Communications Requirements

3.3.1 Core Voice Communications Requirements Overview

Voice Communications Services shall include the following requirements:

1. Enhanced telephony services, including call forwarding, call waiting, programmed directories, teleconferencing, automatic call distribution (useful for busy customer service areas), and call detail recording. Enhanced telephony services should also include precedence and preemption capabilities.

2. Broadcast services that provide one-way audio or audio/video communications services between a sending location and multiple receiving locations. Broadcast services shall also include data communications services.

Voice Communications Services shall provide inter-human voice communications and include real-time and stored voice messages. Telephone services and radio services are specialized forms of voice communications services. An overall voice communications service may actually consist of individual telephone services and radio services. The voice communications services must employ information transfer services in addition to actual voice transmission.

Real-Time voice communications consists of secure and unsecure ship/shore, air/ground and ground/ground voice. In addition a teleconferencing capability provides for secure and unsecure real-time synchronized voice and imagery.

Recorded voice communications, consisting of classified and unclassified recorded messages would be available to dial-in users through any one of a number of commercial off-the-shelf telecommunications processors.

3.3.2 Telephone Services

3.3.2.1 Voice Communications Services shall support 500 type telephones (rotary dial).

3.3.2.2 Voice Communications Services shall support 2500 type telephones (DTMF).

3.3.2.3 Voice Communications Services shall support digital telephone sets with multiple lines.

3.3.2.4 Voice Communications Services shall support digital telephones with multiple keys for special features, display, data capability, etc.

3.3.2.5 Facsimile Services: Voice Communications Services shall support any facsimile machine designed in accordance with EIA Standard RS-465, Group 3 Facsimile Apparatus for Document Transmission.

3.3.3 Voice Communications Services

Voice Communications Services shall provide the following features:

3.3.3.1 Voice Communications Services shall support Call forwarding (all calls / busy, and no answer).

3.3.3.2 Voice Communications Services shall support Call waiting.

3.3.3.3 Voice Communications Services shall support Programmed directories.

3.3.3.4 Voice Communications Services shall support Teleconferencing.

3.3.3.5 Voice Communications Services shall support Automatic call distribution (useful for busy customer service areas).

3.3.3.6 Voice Communications Services shall support Call Park (allows putting a call on hold and disconnecting the call, the call can then be answered from any telephone set).

3.3.3.7 Voice Communications Services shall support Call detail recording.

3.3.3.8 Voice Communications Services shall support Precedence.

3.3.3.9 Voice Communications Services shall support Preemption.

3.3.3.10 Voice Communications Services shall support Hot lines.

3.3.3.11 Voice Communications Services shall support Class-of-service restrictions.

3.3.4 Broadcast Services

3.3.4.1 Voice Communications Services shall support broadcast services that provide one-way audio communications services between a sending location and multiple receiving locations.

3.3.4.2 Voice Communications Services shall support broadcast services that provide one-way digital communications services between a sending location and multiple receiving locations.

3.3.4.3 Voice Communications Services shall be capable of detecting both voice and data when they present on the net.

3.3.5 Visual Services Requirements

3.3.5.1 Teleconferencing Requirements

3.3.5.2 Voice Communications Services shall provide audio teleconferencing with common workstation windows between two or more users. This includes the capability to refresh windows whenever someone displays new material or changes an existing display. Every user is provided the capability to graphically annotate or modify the shared conference window.

3.3.5.3 Voice Communications Services shall provide two-way video transmission between different sites. These services include full motion display of events and participants in a bi-directional manner, support for the management of directing the cameras, ranging from fixed position, to sender directed, to receiver directed, to automated sound pickup.

3.3.5.4 Voice Communications Services shall provide conferencing services that allow groups to participate in conferences. These conferences may not occur in real time. Conferees or invited guests can drop in or out of conferences or subconferences at will. The ability to trace the exchanges is provided. Services include exchange of documents, conference management, recording facilities, and search and retrieval capabilities.

3.4 Information Technical Service Management Requirements

3.4.1 Information Technical Services shall provide the capability to utilize the workstation resident protocol layers over multiple subnetworks.

3.4.2 In addition to the specific layer requirements detailed in subsequent paragraphs, the ISO Reference Model shall be implemented IAW the basic reference model documents and certain layer independent standards as listed below:

3.4.3 Message Handling Capability. Information Technical Services shall:

3.4.3.1 Provide the capability to send formatted messages using the Message Handling System (MHS) protocol as defined in CCITT X.420, CCITT X.411, NIST 500-177, and FIPS PUB 146.

3.4.3.2 Provide the capability to receive formatted messages using the MHS protocol as defined in CCITT X.420, CCITT X.411, NIST 500-177, and FIPS PUB 146.

3.4.3.3 Provide for an MTA multi-destination delivery.

3.4.4 With respect to ISO 8650-1988: Information Processing Systems, Open Systems Interconnection, Protocol Specification for the ACSE,

3.4.4.1 Information Technical Services shall provide Association Control service as defined in ISO 8649/CCITT X.217 and FIPS Pub 146.

3.4.4.2 Information Technical Services shall provide an ACSE protocol as defined in ISO 8650/CCITT X.227, NIST 500-177, and FIPS PUB 146.

3.4.4.3 Information Technical Services shall provide an Association Control Service that supports the "ISO 8650-ACE1" Abstract Syntax as defined in ISO 8650/CCITT X.227, NIST 500-177, and FIPS PUB 146.

3.4.5 With respect to ISO DIS 9066-2.2: Information Processing Systems, Text Communications, Reliable Transfer, Part 2: Protocol Specification, 1989,

3.4.5.1 Information Technical Services shall provide Reliable Transfer service for the MHS protocol as defined in ISO 9066-1.2/CCITT X.218, NIST 500-177, and FIPS PUB 146.

3.4.5.2 Information Technical Services shall provide the RTSE protocol for the MHS protocol as defined in ISO 9066-2.2/CCITT X.228, NIST 500-177, and FIPS PUB 146.

3.4.5.3 Information Technical Services shall provide the Reliable Transfer Service for the MHS protocol that supports the "ISO 9066-RTSE1" Abstract Syntax as defined in ISO 9066-2.2/CCITT X.228, NIST 500-177, and FIPS PUB 146.

3.4.6 Information Technical Services shall provide a Remote Procedure Call (RPC) service IAW ISO DIS 10148-1988 Information Processing Systems Basic RPC Using OSI Remote Operations.

3.4.7 Management. Information Technical Services shall provide the capability for a management service using the Common Management Information Protocol (CMIP) as defined in ISO DIS 9596, FIPS PUB 146, and NIST 500-177.

3.4.8 With respect to ISO DIS 8571-5-1989: Information Processing Systems, Open Systems Interconnection, File Transfer, Access and Management, Part 5: Implementation Conformance Statement Proforma,

3.4.8.1 Information Technical Services shall provide the "FTAM-PCI" Abstract Syntax as defined in ISO 8571-1 to 5, FIPS PUB 146, and NIST 500-177.

3.4.9 With respect to ISO 9041 PDAD2-1989: Information Processing Systems, Open Systems, Interconnection, Virtual Basic Terminal Class Protocol, Addendum 2: Additional Functional Units,

3.4.9.1 Information Technical Services shall provide the capability for terminal emulation in accordance with FIPS PUB 146 and NIST 500-177.

3.4.9.2 Information Technical Services shall provide the "ISO VT" Basic Abstract Syntax as defined in ISO, NIST 500-177, and FIPS PUB 146.

3.4.10 Directory (GOSIP Version 3-1990). Information Technical Services shall provide the capability for the Directory Service as defined in ISO 9594-1 to 8, FIPS PUB 146, CCITT X.500 and NIST 500-177.

3.4.11 Information Technical Services shall provide a Connection Oriented Presentation Service as defined in ISO 8822/CCITT X.216, NIST 500-177, and FIPS PUB 146.

3.4.12 Information Technical Services shall provide a Presentation Protocol Kernel Functional Unit as defined in ISO 8823/CCITT X.226, NIST 500-177, and FIPS PUB 146.

3.4.13 Information Technical Services shall provide a Presentation Service that supports Abstract Syntax Notation One (ASN.1) Transfer Syntax as defined in ISO 8824/CCITT X.208, ISO 8825/CCITT X.209, NIST 500-177, and FIPS PUB 146.

3.4.14 Information Technical Services shall provide a Presentation Service that supports at least three (3) Presentation Contexts as defined in NIST 500-177.

3.4.15 Information Technical Services shall provide the capability to bypass the Presentation protocol kernel functional unit for interoperability with QIP systems provided any security features are not bypassed.

3.4.16 Information Technical Services shall provide the capability for the OSI connectionless transport protocol as defined in ISO 8602, FIPS PUB 146, and NIST 500-177.

3.4.17 Information Technical Services shall provide the capability to send messages using a multicast address.

3.4.18 Information Technical Services shall provide the capability to receive messages using a multicast address.

3.4.19 Information Technical Services shall support the Network Service as defined in ISO 8348 and ISO 8348 Addendum 1 and FIPS PUB 146.

3.4.20 Information Technical Services shall provide the capability for the ES-18

Routing capability defined in ISO 9542, FIPS PUB 146 and NIST 500-177.

3.4.21 Information Technical Services shall provide an open public interface to the DoD host-to-host Services.

3.4.22 Information Technical Services shall have the capability to provide a connection oriented interface to WAN interface devices using the network service primitives as defined in ISO 8348/CCITT X.213.

3.4.23 Information Technical Services shall have the capability to provide a connectionless interface to WAN interface devices using the CLNP primitives as defined in ISO 8348 Addendum 1.

3.4.24 Information Technical Services shall provide the capability to configure particular channels within WAN interface devices with specific, selectable protocols during normal operation of the other physical channels.

3.4.25 Information Technical Services shall provide the capability to initiate transmissions over individual channels selectively within WAN interface devices without affecting the operation and/or state of the other physical channels.

3.4.26 Information Technical Services shall provide the capability to configure and control any communication channel operating parameters for the devices supported by the WAN interface devices without preventing the operation of the other physical channels; this includes device configuration of selected channels, selected channel restart, and selected channel shutdown.

3.4.27 Information Technical Services shall provide the capability to initialize the selected communication protocol within WAN interface devices channels without preventing the operation of the other physical channels.

3.4.28 Information Technical Services shall provide the capability to download subscriber tables to the WAN interfacing devices.

3.4.29 Information Technical Services shall provide the capability to regulate traffic over the Tactical Computer Unit/Portable Computer Unit (TCU/PCU) WAN interfacing devices on a per channel basis without affecting the operation or state of other physical channels.

3.4.30 Information Technical Services shall provide the capability to poll the WAN interfacing devices to ensure a channel is available before transmission.

3.4.31 Information Technical Services shall provide the capability to load the CPP/WAN Interface Devices functions.

3.4.32 Information Technical Services shall provide the capability to control the CPP/WAN Interface Devices functions.

3.4.33 Information Technical Services shall provide the capability to control interfaces to WAN interface devices:

3.4.33.1 Using the network service primitives as defined in ISO 8348/CCIT X.213.

3.4.33.2 Using the CLNP primitives as defined in ISO 8348 Addendum 1.

3.4.33.3 Configuring particular channels within WAN interface devices with specific, selectable protocols during normal operation of the other physical channels.

3.4.33.4 Initiating transmissions over individual channels selectively within WAN interface devices without affecting the operation and/or state of the other physical channels.

3.4.33.5 Configuring any communication channel operating parameters for the devices supported by the WAN interface devices without preventing the operation of the other physical channels. This includes device configuration of selected channels, selected channel restart, and selected channel shutdown.

3.4.33.6 Initializing the selected communication protocol within WAN interface devices channels without preventing the operation of the other physical channels.

3.4.33.7 Downloading subscriber tables to the WAN interfacing devices.

3.4.33.8 Regulating traffic over the Tactical Computer Unit / Portable Computer Unit (TCU/PCU) WAN interfacing devices or a per channel basis without affecting the operation or state of other physical channels.

3.4.33.9 Polling the WAN interfacing devices to ensure a channel is available before transmission.

3.4.34 Control of Internal Communications. Information Technical Services shall have the capability to:

3.4.34.1 Control the Common Management Information Protocol (CMIP) management service.

3.4.34.2 Manage message storage space for safe store and for outgoing traffic until user preset conditions are satisfied.

3.4.34.3 Selectively retrieve message information from the message safe store including default relay information and message status information.

3.4.34.4 Control the substitution of defaults and multihop relay parameters.

3.4.34.5 Monitor the status of message transmission queues, precedence transfers, and multihop relays including the parameters to modify criteria.

3.4.34.6 Monitor status and control mechanisms for communication resources:

1. Create communications resource data log
2. Maintain communications resource data log
3. Review communications resource data log

3.5 Network Services

3.5.1 Network Services Requirements Overview

This section describes the requirements for DII COE data communications. These include the protocols for reliable, transparent, end-to-end data transmission across communications networks. It is divided into the following functional areas:

- Network Communications
- Network Protocols
- Network Applications
- Network Services Defined in Other DII Requirements Specifications

3.5.2 Network Communications

Network Services shall utilize any/all network devices or protocols below the transport layer, as provided by the DII kernel. In addition, Network Services shall support the addition of appropriate device drivers to extend the kernel services as needed.

3.5.2.1 Local Area Network Communications

There are numerous local factors, physical and organizational, that will affect each DII site's local area network (LAN) architecture. Network performance and loading will drive most site architecture decisions. A strategy which should be considered is to isolate workgroups on to subnetworks, reducing the network traffic on the DII site network backbone.

3.5.2.1.1 Network Services shall support IEEE 802.2

3.5.2.1.2 Network Services shall support IEEE 802.3

3.5.2.1.3 Network Services shall support IEEE 802.4

3.5.2.1.4 Network Services shall support IEEE 802.5

3.5.2.1.5 Network Services shall support IEEE 802.11

3.5.2.1.6 In cases where higher network loads are required, FDDI shall be used. This can be used for the whole network or in conjunction with Ethernet

to provide a high speed backbone to support several slower Ethernet subnets.

3.5.2.1.7 ISO 9314 shall be used for the protocols and physical connections for FDDI media access.

3.5.2.1.8 LANs can be connected together by routers to serve a wider community.

3.5.2.2 Metropolitan Area Communications

Metropolitan Area Networks (MANs) link non-contiguous premises within a fixed location. IEEE 802.6 defines a strategy for connecting peer networks together at high speeds using a Dual Queue Dual Bus architecture to support two-way communications.

3.5.2.2.1 IEEE 802.6 shall be supported for connecting DII nodes across a MAN.

3.5.2.3 Wide Area Network Communications

A Wide Area Network (WAN) uses common carrier leased lines or tactical links to connect distant site networks and require additional communications support to cover the distances.

3.5.2.3.1 X.25 shall be supported for connecting DII nodes across a WAN.

3.5.2.3.2 ATM shall be supported for connecting DII nodes across a WAN.

3.5.2.3.3 The Link Access Protocols-Balanced (LAP-B) link protocols shall be used to provide X.25 packet service among DII sites.

3.5.2.4 Dialup Network

3.5.2.4.1 Network Services shall support the PPP protocol.

3.5.2.4.2 Network Services shall support the OSPF-2 protocol.

3.5.2.5 Other Network Communications

Trends for DII requirements are moving towards networked multimedia applications and increasing demands for network services support that can handle greater amounts of data in a shorter time period. The current DII network architecture will have to evolve towards higher speed network communication technologies to support this increased demand for bandwidth.

3.5.2.5.1 Asynchronous Transfer Mode (ATM) provides point-to-point connections between network nodes, giving each pair of stations full network bandwidth. Network Services shall support ATM.

3.5.2.5.2 Fast Ethernet promises to increase the current 10 Mbps Ethernet bandwidth to 100 Mbps. Network Services shall support Fast Ethernet.

3.5.2.5.3 Synchronous Optical Network (SONET) has been developed as a layer 1 and 2 fiber optic transmission service for very high speed facilities. Network Services shall support SONET.

3.5.2.5.4 Broadband Integrated Services Digital Networks (B-ISDN) is a service requiring transmission channels capable of supporting rates greater than the 1.544 Mbps primary rate. It will provide, by using ATM and SONET technologies, interactive and distribution services ranging in bandwidth from 64 Kbps to 644 Mbps. Network Services shall support B-ISDN.

3.5.2.5.5 Frame Relay is a switched service designed to improve communications performance through reduced delays and more efficient bandwidth utilization. Network Services shall support Frame Relay.

3.5.2.5.6 Switched Multimegabit Data Services (SMDS) is an on-demand layer 3 switching service where each frame contains the originating and terminating addresses. Network Services shall support SMDS.

3.5.3 Network Protocols

Network protocols provide network services between platforms on the network. The network protocol standards provide connections, routing, flow control, and data format services for applications to communicate across networks using common protocols without specific knowledge of details of each other's implementation.

3.5.3.1 Network Services shall be based on Transmission Control Protocol / Internet Protocol (TCP / IP), UDP and multicasting.

3.5.3.2 DII COE TCP / IP shall be in compliance with MIL-STD-1778 and MIL-STD-1777 as well as the following RFC's:

- RFC 1123, Requirements for Internet Hosts-Application and Support
- RFC 1122, Requirements for Internet Hosts-Communications Layers
- RFC 1009, Requirements for Internet Gateways.

3.5.3.3 The OSI network protocols shall be supported by Communications Software as specified in the FIPS 146-2 and FIPS 179.1.

3.5.4 Network Applications

Network applications provide standard, common services, building upon the protocols and communications methods that have been previously defined. Some applications which have traditionally been a part of network services, such as Network File System (NFS), are defined by other DII requirements documents (the Distributed Computing Services SRS, in this case). These traditional applications will

be noted here, but will be defined in the DII SRS to which they belong.

3.5.4.1 Electronic Mail (E-mail) Services

E-mail services define the message formats and services for providing message exchange between heterogeneous computer systems in a network environment.

3.5.4.1.1 For DII COE, the Simple Mail Transfer Protocol (SMTP) shall be used. RFC 821 (Message Protocols) and RFC 822 (Text Message Formats) shall be used.

3.5.4.1.2 RFC 1123 shall be used for implementation requirements and updates to RFC 821 and RFC 822.

3.5.4.1.3 The Multipurpose Internet Mail Extensions (MIME) shall be used for moving non-text (i.e., binary files) E-mail within the context of SMTP. RFC 1341 shall be used as the MIME standard.

3.5.4.1.4 Post-Office-Protocol Version 3 (POP-3), as defined by the appropriate RFC, shall be supported.

3.5.4.1.5 The IMAP-4 protocol, as defined by the appropriate RFC, shall be supported.

3.5.4.2 Directory Services

Directory Services allow users to identify, by name, network resources such as servers, files, disks, etc., and gain access to the resource without needing to know where they are located in a network. These requirements are contained within the DII Distributed Computing Services SRS.

3.5.4.3 File Transfer

File transfer services are a set of agreements on procedures that specify how information organized into files can be transferred from one computer to another through homogeneous and heterogeneous networks. These network services provide for the transfer of file data to another location only and do not address data formats or translations which must be accomplished by the source and target systems applications.

3.5.4.3.1 DII COE shall use the File Transfer Protocol (FTP) as specified in MIL-STD-1780. The minimum implementation that is identified in section 4.1.2.13 of RFC 1123 shall be used.

3.5.4.4 Terminal Access

Terminal standards identify services and protocols for remote terminal access to network computing resources.

3.5.4.4.1 MIL-STD-1782, Telnet, shall be used as the standard for simple asynchronous terminal capability.

3.5.4.5 Network Information Discovery and Retrieval

This section describes various applications for use in finding information on the network.

3.5.4.5.1 The Internet Gopher, is a client-server document search and retrieval protocol. The Gopher, as described in RFC 1436, shall be supported.

3.5.4.5.2 HyperText Transport Protocol (HTTP) is a fast search and retrieval protocol used by the World Wide Web (WWW) to transfer HyperText documents from one computer to another. The primary document format is the HyperText Markup Language (HTML). HTTP and HTML shall be supported.

3.5.4.5.3 Network News Transfer Protocol (NNTP) is a protocol for the distribution, inquiry, retrieval, and posting of news articles. The DII COE shall support the NNTP as defined in RFC 977. The format of news articles shall be in accordance with RFC 850, Standard for Interchange of Usenet Messages.

3.5.5 Network Services Applications Defined in Other Requirements Specifications

As a summary, the following network services applications, which have traditionally been a part of network services, are defined in other DII COE SRS:

- Directory Services
- Remote Procedure Calls
- Transparent File Access
- Distributed Authentication
- Network Time Services

The following network services, which have traditionally been a part of network services, are defined in other sections of this SRS (most are in the Distributed Computing Services section):

- Directory Services allow users to identify, by name, network resources such as servers, files, disks, etc., and gain access to the resource without needing to know where they are located in a network.

- Remote Procedure Calls (RPCs) allow applications to invoke procedures that reside on remote hosts.

- Transparent File Access describes standards for sharing and managing data in heterogeneous networks. One example implementation is the Network File System (NFS) Protocol Specification (RFC 1094).

- Distributed Authentication describes how a user is validated to use the resources of the network.

- Time Services: Distributed network systems need a consistent time service. Many distributed services, such as distributed file systems and authentication mechanisms, compare time stamps from different network clients.

3.5.5.1 Remote Procedure Calls (RPCs)

Remote Procedure Calls (RPCs) allow applications to invoke procedures that reside on remote hosts. The requirements are defined in DII Distributed Computing Services SRS.

3.5.5.2 Transparent File Access

Transparent File Access describes standards for sharing and managing data in heterogeneous networks. One example implementation is the Network File System (NFS) Protocol Specification (RFC 1094). Transparent file access requirements are defined in the DII Distributed Computing Services SRS.

3.5.5.3 Distributed Authentication

Distributed Authentication describes how a user is validated to use the resources of the network. Distributed Authentication requirements are defined in the DII Distributed Computing Services SRS.

3.5.5.4 Network Time Services

Distributed network systems need a consistent time service. Many distributed services, such as distributed file systems and authentication mechanisms, compare time stamps from different network clients. Network time services requirements are defined in the DII Distributed Computing Services SRS.

3.5.5.5 Personal / Microcomputer Network Support

Personal microcomputers can be used to access the resources of the DII network. However, they are required to have only a subset of the requirements which have been discussed above. The following sections discuss the requirements for personal computers to connect to DII networks.

3.5.5.5.1 Personal computers shall support a standardized connection to the DII COE networks (Ethernet).

3.5.5.5.2 Personal computers shall support the TCP / IP protocol in order to connect to DII networks.

3.5.5.5.3 All DII personal computer applications shall be Winsock-compliant.

This includes the following network applications:

- E-mail
- File transfer
- Terminal Access
- Network Information Discovery and Retrieval (NIDR)

3.5.5.5.4 Network Services shall provide the heterogeneous interface capability for one system to utilize the network services provided on one platform to communicate with another platform regardless of architectural differences (e.g. big-endian / little endian).

3.6 C4I Communications Services Requirements

The following requirements pertain to C4I systems that are constructed on top of the DII COE framework.

3.6.1 Communications Services shall support Public Switched data Services (PSDS) - Switched 56 Capability.

3.6.2 Communication Services shall support MIL-STD-1553B.

3.6.3 Communication Services shall support MIL-STD-1397A.

3.6.4 C4I Message Management Requirements

3.6.4.1 The system shall be able to bound messages using the rules of the JOTS Header message envelope type.

3.6.4.2 The system shall be able to bound messages using the rules of the ADCCP message envelope type.

3.6.4.3 The system shall be able to bound messages using the rules of the JVMF message envelope type.

3.6.4.4 Support modification of an old message therefore creating a new message by:

1. Retrieving and displaying a whole message;
2. Editing of the displayed message, to include format lines;
3. Replacement of existing addressees;
4. Allowing the revised message to be submitted as a new message.

3.6.4.5 Alternate routes shall be established and canceled by a command that is accessible only by the comms administrator.

3.6.5 C4I Voice Communications Requirements

C4I voice communications services include the following requirements:

Combat Net Radio services that provide audio communications between multiple sending and receiving locations.

The Department of Defense utilizes specialized communications equipment for the purpose of tactical voice communications. The primary formats for voice communications are wide-band 0-25KHZ (UHF Line-of-Sight and SATCOM) and narrow-band (HF USB and SATCOM). There are newer formats (DAMA, SINCGARS, EHF SATCOM, SHF SATCOM, JTIDS) which will play larger roles in DoD voice communications in the future as additional platforms gain these capabilities.

Teleconferencing which provides real-time synchronized voice and imagery is a technology on the horizon for the Department of Defense. This technology is currently being employed utilizing commercial communications paths. In the future DoD SATCOM communications paths will be utilized. The SHF/EHF programs have conducted successful field testing and are proceeding with modifying the cold war nuclear survivable protocols to support extremely high bandwidth (6MHZ uncompressed) multiplexed imagery and voice.

3.6.5.1 Communications Services shall support STU-III telephones.

3.6.5.2 Communications Services shall support KY 68, DSVT, TA-954 DNVT telephones operation at 16 or 32 Kbps.

3.6.5.3 Communications Services shall provide a user interface to select available data rates (up to 1200 baud) for the AN/PRC-77 combat net radio.

3.6.5.4 Communications Services shall provide a user interface to select available data rates (up to 1200 baud) for the AN/PRC-104 combat net radio.

3.6.5.5 Communications Services shall provide a user interface to select available data rates (up to 16k baud) for the SINCGARS combat net radio.

3.6.6 Combat Net Radio

Communications Services shall support Combat Net Radio services that provide audio communications between multiple sending and receiving sites.

3.6.6.1 In the Combat Net Radio network where the voice and data sharing the same net, Communications Services shall withhold the data transmission when the voice Push-to-talk button is activated to prevent voice and data collisions.

3.6.7 C4I Interfaces

DII COE user mail services shall provide message processing that interfaces directly with the user.

3.6.7.1 TADIL-A

3.6.7.1.1 Communications Services shall provide TADIL A services in accordance with MIL-STD-6011A.

3.6.7.1.2 Communications Services shall provide a user interface to configure TADIL-A Link communications.

3.6.7.1.3 Communications Services shall provide a user interface to configure TADIL-A Link forwarding.

3.6.7.1.4 Communications Services shall provide a user interface to monitor TADIL-A link quality.

3.6.7.1.5 Communications Services shall provide a user interface to enter TADIL-A Data Link Reference Point (DLRP).

3.6.7.1.6 Communications Services shall provide a user interface to select and remove TADIL-A track pairing.

3.6.7.1.7 Communications Services shall provide a user interface to support TADIL-A alerts.

3.6.7.2 TADIL-B

3.6.7.2.1 Communications Services shall provide TADIL B services in accordance with MIL-STD-6011A

3.6.7.2.2 Communications Services shall provide a user interface to configure TADIL-B Link communications.

3.6.7.2.3 Communications Services shall provide a user interface to configure TADIL-B Link forwarding.

3.6.7.2.4 Communications Services shall provide a user interface to monitor TADIL-B link quality.

3.6.7.2.5 Communications Services shall provide a user interface to enter TADIL-B Data Link Reference Point (DLRP).

3.6.7.2.6 Communications Services shall provide a user interface to select and remove TADIL-B track pairing.

3.6.7.2.7 Communications Services shall provide a user interface to support TADIL-B alerts.

3.6.7.3 TADIL-J

3.6.7.3.1 Communications Services shall provide TADIL J services in accordance with MIL-STD 6016.

3.6.7.3.2 Communications Services shall provide a user interface to configure TADIL-J Link communications.

3.6.7.3.3 Communications Services shall provide a user interface to configure TADIL-J Link forwarding.

3.6.7.3.4 Communications Services shall provide a user interface to monitor TADIL-J link quality.

3.6.7.3.5 Communications Services shall provide a user interface to select and remove TADIL-J track pairing.

3.6.7.3.6 Communications Services shall provide a user interface to support TADIL-J alerts.

3.6.7.4 TCIM

3.6.7.4.1 Communications Services shall support receipt of OTH-GOLD formatted messages through the TCIM channel.

3.6.7.4.2 Communications Services shall support transmission of OTH-GOLD formatted messages through the TCIM channel.

3.6.7.4.3 Communications Services shall support receipt of binary messages, to include Air Tasking Orders (ATOs), through the TCIM channel.

3.6.7.4.4 Communications Services shall support transmission of binary messages, to include Air Tasking Orders (ATOs), through the TCIM channel.

3.6.7.4.5 Communications Services shall provide a user interface which includes the TCIM as an available communications circuit / interface that may be added.

3.6.7.4.6 Communications Services shall provide a user interface which includes the TCIM as an available communications circuit / interface that may be configured.

3.6.7.4.7 Communications Services shall provide a user interface to identify the tactical communications equipment to be connected to the TCIM channel in accordance with devices which are valid for the channel (including AN / PRC-77, AN / PRC-104, and SINCGARS combat net radios).

3.6.7.4.8 Communications Services shall provide a user interface to select a supported protocol to configure the TCIM channel.

3.6.7.4.9 Communications Services shall provide a user interface to configure the Modulation of the TCIM channel, consistent with the selected protocol and tactical communications equipment.

3.6.7.4.10 Communications Services shall provide a user interface to configure the Data Rate of the TCIM channel, consistent with the selected protocol and tactical communications equipment.

3.6.7.4.11 Communications Services shall provide a user interface to configure the Amplitude of the TCIM channel consistent with the selected protocol and tactical communications equipment.

3.6.7.4.12 Communications Services shall provide a user interface to configure the Subscriber Address of the TCIM channel consistent with the selected protocol and tactical communications equipment.

3.6.7.4.13 Communications Services shall provide error alerts when the operator has made an error in configuring a TCIM channel.

3.6.7.4.14 Communications Services shall provide a user interface to stop a specified TCIM channel.

3.6.7.4.15 Communications Services shall provide a user interface to restart a specified TCIM channel using the latest saved TCIM channel configuration settings.

3.6.7.5 TLC-10

3.6.7.5.1 Communications Services shall provide the capability to transmit formatted messages over the serial channel to the TLC-10.

3.6.7.5.2 Communications Services shall provide the capability to transmit binary messages over the serial channel to the TLC-10.

3.6.7.5.3 Communications Services shall provide the capability to receive formatted messages over the serial channel to the TLC-10 within the existing Communications Services Communication Server architecture.

3.6.7.5.4 Communications Services shall provide the capability to receive binary messages over the serial channel to the TLC-10 within the existing Communications Services Communication Server architecture.

3.6.7.6 PLI

3.6.7.6.1 Communications Services shall correlate PLI updates.

3.6.7.6.2 Communications Services shall store PLI updates.

3.6.7.7 C4I Interface Control

3.6.7.7.1 The Basic Communications Interface Level (BCIL) shall utilize multicast transport services (one-to-many and many-to-one).

3.6.7.8 C4I Network Services

3.6.7.8.1 Introduction

This section contains background information regarding the DII COE network services.

3.6.7.8.2 Dependence Upon DII Management Services SRS

Similarly as with the Distributed Computing Services SRS, there are network management services, for example, Simple Network Management Protocol (SNMP) which are more appropriately discussed within the DII Management Services SRS. The requirements for network management are found in the DII Management Services SRS.

This page intentionally left blank.

Appendix A
Joint and Service Unique Networks

Table A-1 Joint Networks

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
AUTODIN	Serial		Mode 1	USMTF	JANAP 128
TADIL A (LINK 11)	PARALLEL (GET)	OPSPEC 411			
TADIL B					
TADIL J		OPSPEC 416			
CSP	SERIAL				
MCS 11.0					
MTS					
4-WIRE	SCSI (TCIM)	MIL-STD-188-220			
2-WIRE	SCSI (TCIM)				
AFATDS					
ITW/AA					
TACFIRE	CNR	FS INITIAL ACCESS INTERFACE	FSAC FIRE SUPPORT (FS)		
	WIRELINE				
	CNR	FS INITIAL ACCESS INTERFACE	IFSAS FIRE SUPPORT (IFS)		
	WIRELINE				

Table A-1 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
	CNR	FS INITIAL ACCESS INTERFACE	IFS ENHANCED		
	WIRELINE				
	CNR	tbd	IFS SMART		
	WIRELINE				
	WIRELINE	tbd	GUN DIRECTION UNIT (GDU)		
	WIRELINE	tbd	NATO STANAG 5620		
JOINT	CNR	tbd	JVMF (MIL-STD 188-220) (1993)		
	WIRELINE				
	KG-84A				
	DSVT				
	DNVT				
	2WIRE-4WIRE				
	CNR	tbd	MIL-STD 188-220(A) (1995)		
	WIRELINE				
AFATDS	CNR	tbd	AFATDS FIRE SUPPORT (AFS)		
	WIRELINE				
	CNR	tbd	MLRS		
	WIRELINE				

Table A-1 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
MARINE CORPS	CNR	MTS TIDP	MARINE TACTICAL SYSTEMS (MTS)		
	WIRELINE				
	DSVT				
	DNVT				
	2WIRE-4WIRE				
	CNR	MTS TIDP	MARINE TACTICAL SYSTEMS (MTS) VERSION 5		
	WIRELINE				
	DSVT				
	DNVT				
	2WIRE-4WIRE				
	tbd	MTS MODE 7	MARINE TACTICAL SYSTEMS SWITCHED (ULS)		
RADIO	CNR	DWG NO C157069	NETWORK RADIO PROTOCOL (NRP) (FOR B2C2/INTEL)		
	WIRELINE				
	CNR	MIAR RIU APPENDIX 1 (SB-SA1A210)	TANK NETWORK RADIO PROTOCOL (NRPT)		
	WIRELINE				

Table A-1 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
	CNR	IEW IDD	IEW COMCAT (FOR B2C2 / INTEL)		
	WIRELINE				
	CNR	tbd	SIMPLE MODEM CNR		
		FDL TIDP SINCGARS BROADCAST NET APP 30 TO MIS 36264	FDL SINCGARS (BROADCAST NET)		
	CNR	MIAR RIU APPENDIX 1 (SB-SA1A210)	NRPT AWE (ARMY WAR-FIGHTING EXP.)		
	WIRELINE				
	CNR	tbd	AIR DEFENSE INTERFACE (ADI) (TADILB / ATDL 1)		
	CNR	tbd	VARIABLE MESSAGE FORMAT (VMF)		
	WIRELINE				
	KG-84A				
	DSVT				
	DNVT				
	2WIRE-4WIRE				
ADDS	ADDS PJHI	tbd	ARMY DATA DISTRIBUTION SYSTEM (ADDS)		
	AFATDS PJHI (EPLRS)				
	MPN				

Table A-1 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
MPN	CONDITION DI-PHASE	SR-43	MSE X.25		
	ETHERNET	SR-45	IEEE 802.3		
ALL	SCSI	tbd	SINCGARS RADIO CONTROL		
	2WIRE				
JOINT	CNR	tbd	JVMF (MIL-STD- 188-220) (1993)		
	WIRELINE				
	KG-84A				
	DSVT				
	DNVT				
	2WIRE-4WIRE				
	CNR	tbd	MIL-STD 188-220(A) (1995)		
	WIRELINE				
	WIRELINE	tbd	NATO STANAG 5620		

Table A-2 Joint Networks

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
JTIDS EPLRS	NRZ CDP	ACCS-A3-407-008C	ADDS	ALL	
COMBAT NET RADIO (SINCGARS, AN/PRC-104, AN/GRC-213, AN/GRC-193, AN/PRC-77, etc.	NRZ FSK-188B FSK-188C STANAG 4202	MIL-STD-188-114A MIL-STD-188-110 STANAG4202 CSESD-14G (C) ITT-AOD-No. 337032004-2	MTS, MTS Version V, NRP, NRPT, NRPT(AWE, CMT, AFATDS FS(AFS) Fire Support, IFSAS, IFSAS Enhanced, IFS Smart, MIL-STD-188-220, SINCGARS 2-2-2, MIL-STD-188-220A	ALL	
MSE Circuit Switch (DNVT/DSVT)	NRZ	MIL-STD-188-114A, TT-B1-4001-0014, TT-C1-7205-0102, TT-B1-4204-0028B, TT-A3-9013-0048B	MSE Circuit Switch	ALL	
SB-3614(V)/ TT Circuit Switch	STANAG 4202	MIL-S-29354	MTS Switched (ULS)	ALL	
AN/GYC-7/ (Wireline, KG-84)	NRZ CDP	MIL-STD-188-114A, ACCS-A3-407-008C, TT-C1-7204-0099	MTS TIDP MODE VII	ALL	

Table A-2 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
MIL-STD-188-220/ (2-wire, CNR, KG-84, DSVT, DNVT, SB-3614A, SB-3865, STU-III	NRZ, FSK-188B, FSK-188C, STANAG 4202, CDP, DPSK	MIL-STD-188-114A, MIL-STD-188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No.337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B	MIL-STD-188-220, JVMF, TCP/IP, UDP	VMF TIDP (TE)	
MIL-STD 188-220A/ (2-wire, 4-wire, CNR, KG-84, DSVT, DNVT, SB-3614A,SB-3865, STU-III, INC, SIP)	NRZ, FSK (Voice), FSK (Single Ch. Radio), Conditioned Diphase, DPSK (Voice), Packet Mode, Amplitude Shift Keying (ASK)	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, CCITT X.21, CCITT V.10, ITT-AOD-No. 337032004-2 CSESD-14G (C), EIA-RS-232	MIL-STD 188-220A, TCP/UDP, IP, PPP	VMF TIDP (TE)	
MSE Packet Switch (LAN/4-wire)	CDP, LAN	SR-43A, SR-45A	DDN X.25, TCP/UDP, IP		

Table A-2 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
TACFIRE/ (2-wire, 4-wire, CNR, KY-57, KG-84, DSVT, DNVT, SB-3614A, SB-3865,)	NRZ, FSK-188B, FSK-188C, STANAG 4202, CDP	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, CSESD-14G	Fire Support, IFSAS, IFSAS Enhanced, IFSAS Smart	ALL	
MTS/ (2-wire, 4-wire, CNR, KY-57, KG-84, DNVT, DSVT,SB-3614A, SB-3865)	NRZ, CDP, FSK-188B, FSK-188C, STANAG 4202, MIL-STD-188-110A	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, TT-B1-1201-0030B, CSESD-14G	MTS		

Table A-2 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
MTS Version 5/ (2-wire, 4-wire, CNR, KY-57, KG-84, DNVT, DSVT,SB-3614A, SB-3865)	NRZ, CDP, FSK-188B, FSK-188C, STANAG 4202, MIL-STD-188-110A	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, TT-B1-1201-0030B, CSESD-14G	MTS Version 5	ALL	
Net Radio Protocol (NRP)/ (2-wire, 4-wire, CNR, KY-57, KG-84)	NRZ, CDP, FSK-188B, FSK-188C, STANAG 4202, MIL-STD-188-110A	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, TT-B1-1201-0030B, CSESD-14G	Net Radio Protocol		

Table A-2 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
Tank Net Radio Protocol (TNRP) / (2-wire, 4-wire, CNR, KY-57)	NRZ, CDP, FSK-188B, FSK-188C, STANAG 4202, MIL-STD-188-110A	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, TT-B1-1201-0030B, CSESD-14G	NRPT, NRPT (AWE)	ALL	
IEWCOMCAT/ (2-wire, 4-wire, CNR, KY-57, KG-84, DNVT, DSVT, GRA-39)	NRZ, CDP, FSK-188B, FSK-188C, STANAG 4202, MIL-STD-188-110A	MIL-STD 188-114A, MIL-STD 188-110, ACCS-A3-407-008C, STANAG 4202, MIL-S-29354, ITT-AOD-No. 337032004-2, TT-B1-4204-0028B, TT-A3-4001-0014, TT-C1-7205-0102, TT-A3-9013-0048B, TT-C1-7204-0099, CSESD-14G	IEWCOMCAT		
TADIL-B/DNVT	NRZ	SR-RG-83-9-C	Air Defense Interface Protocol	ALL	
ATDL-1/DNVT	NRZ	SR-RG-83-9-C	Air Defense Interface Protocol	ALL	

Table A-2 Joint Networks (Continued)

Network/ Interface	Interface Type	Interface Spec	Protocol	Message Type	Message Bounding
TADIL (LINK 11)	TBD	STANAG 4312, MIL-STD-188-212	FAADC2I Data Link	TBD	
TIBS		TDIMF Rev. B #G4097.00.37			
TADIL J	TBD	STANAG 4312	FAADC2I Data Link	TBD	

NAVY/MARINE CORPS NETWORKS

Table A-3 Navy/Marine Corps Networks

Network/ Interface	Interface Type	Interface Spec.	Protocol	Message Type	Message Bounding
POST					
OTCIXS	Serial	IDS 8648	Async	OTH-T Gold	“JOTS”
SSIXS		IRS Dated 26 MAR 1991			
JMIE					
LINK 14	SERIAL	OPSPEC 414			
ACDS	PARALLEL	IDS CSE-KQ-9101			
ADS/JMCIS		WS19702			
CVNS		T9427-AB-IDS-010/CVNS			
SPA-25G		IRS 4E1-1116.6W			
RAYCAS V					
TACINTEL		IDS Dated 30 DEC 1985			

Appendix B

Communications Services APIs

API	Reference Document
addline	JMCIS Comms
appendline	JMCIS Comms
VCloseIcm	JMCIS Comms
VCloseOcm	JMCIS Comms
VIcmAppendLog	JMCIS Comms
VIcmAppendMsg	JMCIS Comms
VIcmChanStat	JMCIS Comms
VIcmDeleteLog	JMCIS Comms
VIcmLogHdr	JMCIS Comms
VIcmPending	JMCIS Comms
VIcmReadMlog	JMCIS Comms
VIcmReadTail	JMCIS Comms
VIcmReceiveNotify	JMCIS Comms
VIcmSetMode	JMCIS Comms
VIcmSetTypes	JMCIS Comms
VIcmUpdateField	JMCIS Comms
VIcmUpdateLog	JMCIS Comms
VMsgFile	JMCIS Comms
VOcmAppendLog	JMCIS Comms
VOcmAppendMsg	JMCIS Comms
VOcmChanStat	JMCIS Comms

API	Reference Document
VOcmDeleteLog	JMCIS Comms
VOcmLogHdr	JMCIS Comms
VOcmPending	JMCIS Comms
VOcmReadMlog	JMCIS Comms
VOcmReadTail	JMCIS Comms
VOcmReceiveNotify	JMCIS Comms
VOcmSetMode	JMCIS Comms
VOcmSetTypes	JMCIS Comms
VOcmUpdateField	JMCIS Comms
VOcmUpdateLog	JMCIS Comms
VOpenIcm	JMCIS Comms
VOpenOcm	JMCIS Comms
VXmitBinFile	JMCIS Comms
VXmitBinFiles	JMCIS Comms
VXmitFile	JMCIS Comms
VXmitFiles	JMCIS Comms
VXmitMsg	JMCIS Comms
VXmitMsgs	JMCIS Comms

Appendix C

Communications Services Internal Interfaces

Acronyms and Abbreviations

AC	Access Control
ACK	Acknowledgment
ACP	Allied Communications Publication
ADPE	Automatic Data Processing Equipment
AE	Authentication Exchange
AIG	Address Indicator Group
AIS	Automated Information System
AMHS	Automated Message Handling System
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile
APSE	Ada Programming Support Environment
ASC	American Standards Committee
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASSET	Asset Source for Software
ATM	Asynchronous Transfer Mode
AUTODIN	Automated Data Information Network
BLOB	Binary Large Object
BMP	Bitmapped picture

C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
CAD	Computer-Aided Design
CASE	Computer-Aided Software Engineering (See ISEE)
CCB	Configuration Control Board
CCIP	Command Center Initiatives Program
CCITT	Consultative Committee on International Telegraph and Telephone
CDA	Computer Design Activity
CFA	Center for Architecture
CFE	Center for Engineering
CFII	Center for Integration & Interoperability
CFS	Center for Standards
CIM	Corporate Information Management
CINC	Commander-in-Chief
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLNP	Connectionless Network Protocol
CMIS/P	Common Management Information Services and Protocols
CMW	Compartmented Mode Workstation
CN	Communications Network
COE	Common Operating Environment
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COTS	Commercial-off-the-Shelf
CRT	Cathode Ray Tube
CTE	Center for Test and Evaluation
CTOS	Convergent Technologies Operating Systems
CTT	Commander's Tactical Terminal
DMS	Defense Message System

DNS	Domain Name Service
DoD	Department of Defense
DA	Data Administrator
DAA	Designated Approving Authorities
DAPM	Domain Analysis Process Model
DAPMO	Data Administration Program Management Office
DARIC	Defense Automation Resources Information Center
DASD (IM)	Deputy Assistant Secretary of Defense for Information Management
DBA	Database Administration
DBMS	Database Management System
DCE	Distributed Computing Environment
DDI	Director of Defense Information
DDL	Data Definition Language
DEPSECDEF	Deputy Secretary of Defense
DGSA	Defense Goal Security Architecture
DI	Date Integrity
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISC	Defense Information System Council
DISSP	Defense Information System Security Program
DITPRO	Defense Information Technical Procurement Office
DMF	Data Management Facility
DMRD	Defense Management Review Decision
DNS	Domain Name Server
DNSIX	DODIIS Network Security for Information Exchange
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction

DODIIS	DoD Intelligence Information System
DODM	DoD Manual
DS	Digital Signature
DSN	Defense Switched Network
DSRS	Defense Software Repository System
DSS	Digital Signature Standard
DSSSL	Document Style Semantics and Specification Language
DTD	Document Type Definition
DTMP	Data Communications Protocol Standards Technical Management Panel
E	Encipherment
E-mail	Electronic Mail
EAD	Executive Agent Developer
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce, and Transportation
EEI	External Environment Interface
EPLRS	Enhanced Position Location Reporting System
ES	End System
FAPM	Functional Activity Program Manager
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FOC	Full Operational Capability
FTP	File Transfer Protocol
FY	Fiscal Year
GBS	Global Broadcast System
GCCS	Global Command and Control System
GCSS	Global Command Support System
GNMP	Government Network Management Profile

GOSIP	Government Open System Interconnection Profile
GOTS	Government Off-the-Shelf
GUI	Graphical User Interface
HCI	Human Computer Interface
HTML	Hypertext Markup Language
HYTIME	Hypermedia/Time-Based Structuring Language
I&RTS	Integration and Runtime Specification
I/O	Input/Output
ICCCM	Inter-Client Communications Conventions Manual
IDD	Interface Design Document
IDS	Interface Design Specification
ICASE	Integrated Computer Aided Software Engineering
IEEE	Institute of Electrical and Electronic Engineers
IEMATS	
IETM	Interactive Electronic Technical Manual
IGES	Initial Graphics Exchange Specification
IGOSS	Industry/Government Open System Specification
IM	Information Management
IMS	Information Management System
INCA	Intelligence Communications Architecture
INRI	International Research Institute
INX	Information Exchange
IP	Internetwork Protocol
IRAC	International Requirements and Design Criteria
IRDS	Information Resource Dictionary System
IRS	Interface Requirements Specification
IS	Information System
ISA	Information System Architecture
ISB	Intelligence Systems Board

ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment
ISO	International Standards Organization
IT	Information Transfer
ITPB	Information Technology Policy Board
ITRUS	Information technology reuse
JANAP	Joint Army, Navy, Air Force Publication
JCS	Joint Chief of Staff
JIEO	Joint Interoperability and Engineering Organization
JMCIS	Joint Maritime Command Information System
JVMF	Joint Variable Message Format
JOTS	Joint Operation Tactical System
JTC	Joint Technical Committee
JTC3A	Joint Tactical Command, Control and Communications Agency
JTT	Joint Tactical Terminal
JVMF	Joint Variable Message Format
LAN	Local Area Network
LAPB	Link Access Protocol B
LCM	Life Cycle Management
LCM	Life Cycle Model
LDMX	Local Digital Message Switch
LSE	Local Subscriber Environment
MATT	Multimission Advanced Tactical Terminal
MHS	Message Handling System
MIS	Management Information Systems
MLS	Multilevel Security
MOA	Memorandum of Agreement

N	Notarization
NACK	Negative Acknowledgment
NATO	North Atlantic Treaty Organization
NCA	National Command Authority
NCCS	Navy Command and Control System
NCCOSC	Navy Command, Control and Ocean Surveillance Center
NCSC	National Computer Security Center
NDI	Non-Development Items
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NRaD	Navy Command, Control and Ocean Surveillance Center Research and Development
NSA	National Security Agency
NSD	National Security Directive
NSRD	National Software Reuse Directory
NTIS	National Technical Information Service
NVLAP	National Voluntary Laboratory Accreditation Program
OASD	Office for the Assistant Secretary of Defense
ODA	Office Document Architecture
ODIF	Office Document Interchange Format
ODL	Office Document Language
ODM	Organizational Domain Modeling
OIW	OSI Implementors' Workshop
OODBMS	Object-Oriented Database Management System
ORB	Object Request Broker
OS	Operating System
OSD	Office of the Secretary of Defense
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection

OTCIXS	Officer-in-Tactical-Command Information Interchange System
OTH-T	Over-The-Horizon Targeting
OTI	Office of Technical Integration
PCIS	Portable Common Interface Set
PCTE	Portable Common Tools Environment
PDES	Product Data Exchange using STEP
PEX	PHIGS Extension to X Windows
PHIGS	Programmer's Hierarchical Interactive Graphics System
PLA	Plain Language Addressee
PLRS	Position Location Reporting System
PMP	Program Management Plan
POSIT	
POSIX	Portable Operating System Interface (for Computer Environments)
PSA	Principal Staff Assistant
PSDS	Public Switched Data Service
RC	Routing Control
RDA	Remote Database Access
RDBMS	Relational Database Management System
RI	Routing Indicator
RLF	Reuse Library Framework
ROAMS	Reusable Object Access and Management System
RPC	Remote Procedure Call
RS	Relay System
SAME	SQL Ada Module Extensions
SAMeDL	SQL Ada Module Extension Description Language
SAMP	Security Association Management Protocol
SBIS	Sustaining Base Information Architecture Framework

SCSI	Small Computer System Interface
SDD	System Design Document
SDNS	Secure Data Network System
SECDEF	Secretary of Defense
SGML	Standard Generalized Markup Language
SII	System Internal Interfaces
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRS	Subsystem Requirements Specification
STARS	Software Technology for Adaptable Reliable Systems
STEP	Standard for the Exchange of Product Model Data
STM	Synchronous Transfer Mode
SWG	Special Working Group
TA	Technical Architecture
TADIL	Tactical Data Link
TADIXS	Tactical Data Interchange System
TAFIM	Technical Architecture Framework for Information Management
TBD	To Be Determined
TCIM	Tactical Communications Interface Module
TCIS	TCIM Common Interface Software
TCP	Transport Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDI	Trusted Database Interpretation
TFA	Transparent File Access
TIBS	Tactical Information Broadcast Service
TIM	Technical Integration Manager
TLSP	Transport Layer Security Protocol

TNI	Trusted Network Interpretation
TP	Traffic Padding
TRE	Tactical Receiving Equipment
TRM	Technical Reference Model
TRI-TAC	Tri-Service Tactical Communications Systems
TSIG	Trusted Systems Interoperability Group
UDP	User Datagram Protocol
UI	UNIX International
UIDL	User Interface Definition Language
UIMS	User Interface Management System
UISRM	User Interface System Reference Model
USMTF	United States Message Text Format
VME	
VMF	Variable Message Format
WAN	Wide Area Network